OUTCOME 4

METHODOLOGY TO UNDERSTAND INTER-DOMAIN DEPENDENCIES & VULNERABILITIES

GUIDE V. 1.0

31 January 2013

U.S.-CREST

FONDATION
pour la RECHERCHE
STRATÉGIQUE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **08 JUL 2013**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE **Multinational Experiment 7 OUTCOME 4 UNDERSTANDING INTER-DOMAIN DEPENDENCIES & VULNERABILITIES CONCEPTUAL AND PRE-DOCTRINAL PAPER 31 JANUARY 2013**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

This document aims to capture some of the conceptual and pre-doctrinal considerations developed in the context of MNE 7 Outcome 4 related to Inter-Domain Understanding. Although the focus of MNE 7 Outcome 4 was on the development of a methodology to identify inter-domain dependencies and related vulnerabilities, a number of broader considerations emerged in support of this methodology. They are encapsulated here. It is important to note that unless specified, the considerations described in this paper have not been subject to experimentation during MNE 7.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	**UU**	**54**	
unclassified	**unclassified**	**unclassified**			

DISTRUBUTION STATEMENT

Table of Contents

Tables and Figures

Intentionally Blank

Table of Abbreviations

A2	Air Intelligence
A2/AD	Anti-Access and Area Denial
AD	Air Defense
AI	Air Interdiction
AIS	Automatic Identification System
AOO	Area of Operation
BLOS	Beyond Line of Sight
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAOC	Combined Air and Space Operations Center
CC	Critical Capability
CDL	Common Data Link
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIMIC	Civil-Military Co-Operation
CJFHQ	Combined Joint Force Headquarters
CNA	Computer Network Attack
CNI	Computer Network Intelligence
CNO	Computer Network Operation
COA	Courses of Action
CoG	Center of Gravity
COP	Common Operational Picture
CR	Critical Requirement
CSAR	Combat Search and Rescue
CV	Critical Vulnerability
CWAN	Coalition Wide Area Network
DCA	Defensive Counter-Air
DIME	Diplomatic, Information, Military, and Economic
DoS	Denial of Service
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Interoperability
ECOA	Enemy Courses of Action
ELINT	Electronic Intelligence
EUTELSAT	European Telecommunications Satellite Organization
EW	Early Warning
F2T2EA	Find, Fix, Track, Target, Engage, Assess
FMV	Full Motion Video
FoN	Freedom of Navigation
GBS	Global Broadcast Service
GPS	Global Positioning System

HALE	High Altitude Long Endurance
HQ	Headquarters
IADS	Integrated Air Defense Systems
ID	Inter-Domain
IDWG	Inter-Domain Working Group
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
J2	Joint Intelligence
JFACC	Joint Force Air Component Commander
JFHQ	Joint Force Headquarters
JOA	Joint Operations Area
JPG	Joint Planning Group
JSTARS	Joint Surveillance and Target Attack Radar System
JTAC	Joint Terminal Attack Controller
JTIDS	Joint Tactical Information Distribution System
KD	Knowledge Development
Kmap	Knowledge Map
LCC	Land Component Commander
LOS	Line of Sight
MALE	Medium Altitude Long Endurance
MCC	Maritime Component Commander
MET	Mission Essential Task
MILSATCOM	Military Satellite Communications
MOC	Maritime Operations Center
MPE	Mission Planning Environment
N2	Naval Intelligence
NCAGS	Naval Co-operation and Guidance for Shipping
NEO	Non-Combatant Evacuation Operations
NTM	National Technical Means
OCA	Offensive Counter-Air
PGM	Precision-Guided Munitions
PMESII	Political, Military, Economic, Social, Information, and Infrastructure
PNT	Positioning, Navigation, and Timing
POE	Preparation of the Operational Environment
RADINT	Radar Intelligence (from Non-Imaging Radar)
RCC	Regional Combatant Command
RF	Radio Frequency
SA	Situational Awareness
SAR	Satellite Synthetic Aperture Radar
SATCOM	Satellite Communications
SEAD	Suppression of Enemy Air Defenses
SIGINT	Signals Intelligence
SLOC	Sea Line of Communication

SOV	System Operational View
SPOD	Sea Ports of Debarkation
SSN	Submersible Ship - Nuclear
TADIL-J	Tactical Digital Information Link Joint
UAS	Unmanned Aircraft System
UFO	UHF Follow-On
UHF	Ultra-high Frequency
WGS	Wideband Global SATCOM

Intentionally Blank

Executive Summary

1. Introduction

This guide provides a methodology and some associated products that could be used to **complement** existing **intelligence preparation of the operational environment (POE)**, **knowledge development (KD) and operational planning processes** by providing **an inter-domain perspective**.

"**Inter-domain**" is the adjective qualifying something which is related to two or more different domains (land, maritime, air, space and cyber).

Although this guide was developed within the context of Multinational Experiment 7 (MNE 7), which is focused on access to the Global Commons (defined as specific portions of the maritime and air domains, as well as the space and cyber domains), the methodology takes a broader view of inter-domain challenges by considering the land domain and the entirety of the domains mentioned above.

Understanding interactions among domains is increasingly important for most engagements, given the level of reliance of traditional joint or domain-specific (land, maritime and air) operations on space and cyber-based capabilities combined with the level of sophistication of the means available to hostile actors, particularly their ability to affect the cyber and space domains.

This guide is primarily intended for **operational-level commanders and their staffs in order to improve their understanding of inter-domain issues.** It contains **a methodology to analyze inter-domain relationships, dependencies and vulnerabilities,** which is intended to enable a **better integration of space and cyber operational issues** in support of mission analysis and course of action development within the operational planning process. The methodology may be implemented during standing strategic awareness, but is primarily designed to support contingency planning and crisis response planning within existing knowledge development (KD)/intelligence and planning processes.

The NATO Comprehensive Operations Planning Directive (COPD) and the Military Decision-Making Process-Multinational (MDMP-M) were used as a backdrop for the development of the methodology. However, the methodology is meant to be easily adaptable to various decision-making processes.

The methodology is focused primarily on the identification of a coalition's potential inter-domain vulnerabilities but it is assumed that it could also be applied to the analysis of an adversary's vulnerabilities. It is also assumed that the implementation of the guide requires bringing together intelligence and/or knowledge development expertise, planning expertise (J5, J3 and J6) as well as cyber and space expertise, through local liaison or reach back.

This guide should be read in conjunction with the MNE 7 Outcome 4 Conceptual and Pre-Doctrinal Paper: "Understanding Inter-Domain Dependencies and Vulnerabilities", which provides additional information regarding the military problem that inter-domain understanding address, proposes a conceptual framework to develop this understanding and addresses potential DOTMLPFI implications.

2. Summary of the Methodology

The inter-domain (ID) methodology consists of three iterative modules, which, based on the modeling of the "ID System" of a given engagement (as defined in the appendix B), enable the identification of critical inter-domain vulnerabilities. These modules and their interactions with the decision-making process may be summarized as follows:

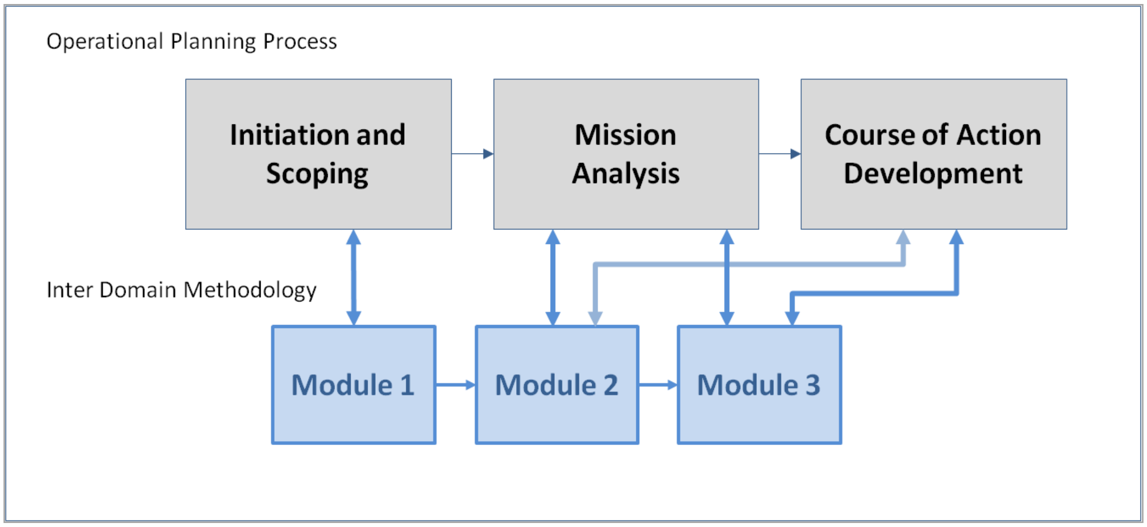


Figure 1 - Interactions between the Modules and the Decision-Making Process

- **Module 1: Framing the inter-domain dimension of the engagement**. This module aims to identify the inter-domain issues in the engagement space, as well as the military functions, the non-military domain functions, and the capabilities to be taken into account in order to orient subsequent steps of the methodology. It is an integral part of the problem framing undertaken at the beginning of the operational planning process.

- **Module 2: ID relationships mapping and ID dependencies analysis.** The aim of this module is to map the inter-domain relationships between the elements and to understand the critical inter-domain dependencies. The level of detail at which the mapping and analysis is performed depends on the time available to develop the preparation of the operational environment (POE) and on information on hand regarding Blue (partners) and Green (non-aligned actors) capabilities and resources.

- **Module 3: Critical ID vulnerabilities identification**. In this module, the analysis and correlation of the direct and indirect effects that would result from an attack or a hazard on vulnerable systems representing critical ID dependencies leads to the identification of the critical ID vulnerabilities.

Modules 2 and 3 should be applied at two separate stages of the operational planning process:

- First, during mission analysis to contribute to a cross-functional analysis of the center of gravity. This work complements the analysis of the CoG critical capabilities, critical requirements and critical vulnerabilities. This analysis also feeds the development of the ECOAs.
- Second, in support of course of action (COA) development drawing predominantly on the Enemy COAs developed through the POE process and the initial COAs developed by the joint planning group. This involves updating the critical dependencies and vulnerabilities for the different COAs based on the dynamics of the engagement. The analysis of the critical ID vulnerabilities should be also refined as part of the COA gaming given that action/reaction/counter-reaction analysis may highlight new unexpected critical ID vulnerabilities that were not previously identified. This analysis then feeds the risk analysis for the Blue COAs and the development of risk mitigation options.

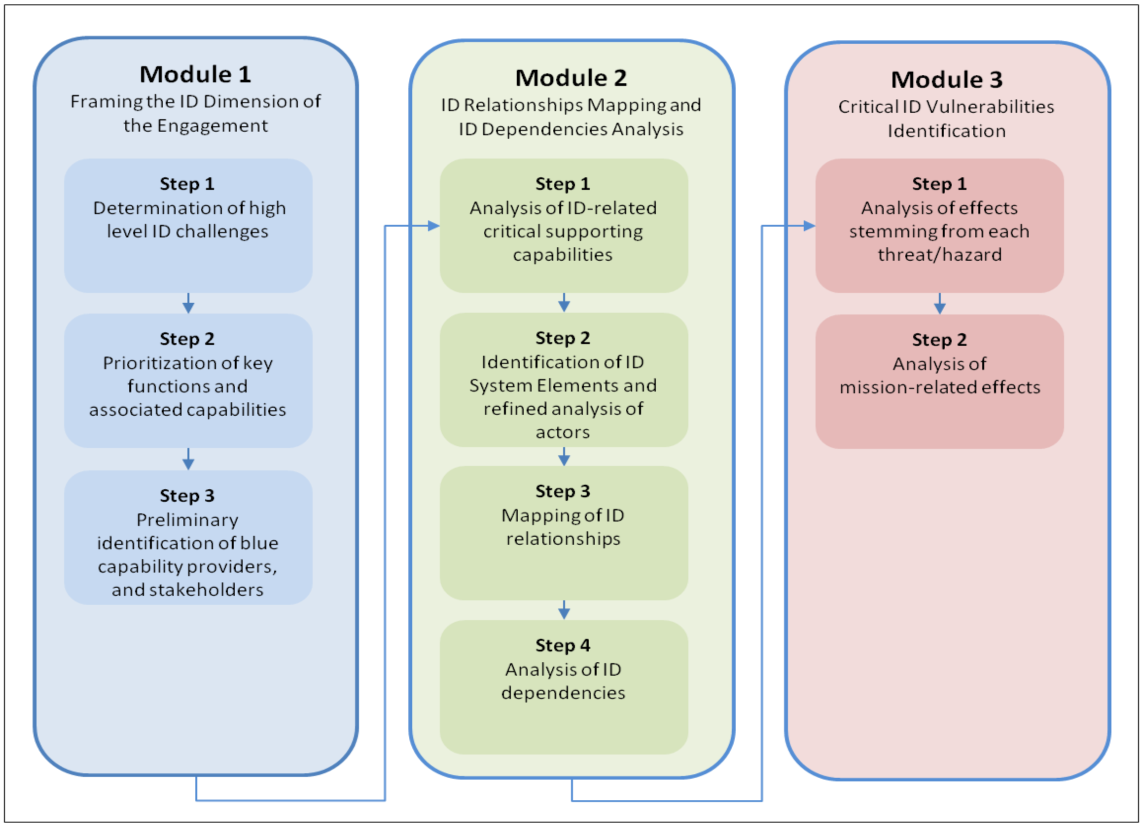

Module 1
Framing the ID Dimension of the Engagement
Step 1
Determination of high level ID challenges
Step 2
Prioritization of key functions and associated capabilities
Step 3
Preliminary identification of blue capability providers, and stakeholders
Module 2
ID Relationships Mapping and ID Dependencies Analysis
Step 1
Analysis of ID-related critical supporting capabilities
Step 2
Identification of ID System Elements and refined analysis of actors
Step 3
Mapping of ID relationships
Step 4
Analysis of ID dependencies
Module 3
Critical ID Vulnerabilities Identification
Step 1
Analysis of effects stemming from each threat/hazard
Step 2
Analysis of mission-related effects

Figure 2 – Step-by-Step View of the Modules

3. Conceptual Models and Proposed Tools Associated with the Methodology

The implementation of this methodology may draw on the **conceptual models** proposed in appendices B and D (inter-domain functional models and explanation of key terms). Furthermore, although computer tools are not required to apply the methodology, some may nonetheless greatly facilitate its implementation by saving time during the decision-making process. Three types of computer-related **tools** in particular are discussed in appendix C:

- A systems database and associated systems operational views;
- A tool to facilitate the development of the knowledge maps (Kmaps);
- An ontology tool.

3.1 Conceptual Models

Appendix D provides the intellectual underpinnings of the methodology. It defines the **key terms** to be used to consider ID issues, explains the linkages between them and provides a way to visualize them.[1]

The **inter-domain functional models** described in appendix B are intended to provide a generic ID perspective of the capabilities and related systems and assets for each military function or non-military domain function; drawing on these models should facilitate the identification of the key systems and assets.

3.2 Computer-Related Tools

The methodology imagines the development of an **"ID systems database"** and a tool that would enable the conversion of the elements within the database into **systems operational views (SOVs)**. The purpose of the database would be to make the information regarding certain standing inter-domain relationships readily available; the purpose of the SOVs would be to capture and support the visualization of the inter-domain relationships among key systems or assets. The structure of such an "ID systems database" is proposed in this guide; ideally, if potential force contributing nations or alliances developed this type of database during peacetime, then shared the relevant information when planning for a specific operation, they would be able to save a great deal of time during operational planning.

The guide also proposes the development of **knowledge maps** (Kmaps), as a way to depict and analyze inter-domain relationships and dependencies. While Kmaps can be drawn manually or using basic software tools, their development would again be greatly facilitated by the use of a computer tool, ideally one connected to the database and systems operational views described above. Appendix C therefore also includes some recommendations regarding requirements for a potential tool that would assist in the development of Kmaps.

The guide furthermore addresses the use of **ontology tools,** although they are not directly incorporated into the methodology. These tools, which include a database of classes (key terms), and semantic linkages, and a "reasoner" tool, may support the methodology by inferring relationships between actors, functions, systems, system elements, etc.

***

[1] For more detail on this conceptual framework please refer to the MNE7 Outcome 4 Conceptual and Pre-Doctrinal Paper: Understanding Inter-Domain Dependencies and Vulnerabilities, dated 31 January 2013.

Introduction

The material presented in this guide seeks to **complement** existing **intelligence preparation of the operational environment (POE)**, **knowledge development (KD) and operational planning processes** by **providing an inter-domain perspective**.

1. Context

Understanding inter-domain (ID) interactions is increasingly important for most engagements, given the following trends:

- The increasing level of reliance of traditional joint or domain specific (land, maritime and air) operations on space and cyber capabilities. This reliance is particularly critical when an engagement requires a strong level of interaction and synergy between the activities planned in the different traditional domains (both joint and component specific).
- The level of sophistication of the means available to potential hostile actors, particularly their ability to affect the cyber and space domains. Dynamics such as the emergence of hybrid threats or the risk of conventional conflicts involving regional and emerging powers who are well-equipped with anti-access and other sophisticated assets will probably reinforce the criticality of inter-domain issues in future engagements.

2. Purpose of the Guide

This guide is primarily intended for **operational-level commanders and their staffs in order to improve their understanding of inter-domain issues.** It contains a methodology to consider inter-domain relationships, dependencies and vulnerabilities (See appendix D for the definitions of the key terms used in this guide). The methodology is composed of three “modules”:

- Module 1: Framing the inter-domain dimension of an engagement;
- Module 2: ID relationships mapping and ID dependencies analysis;
- Module 3: Critical ID vulnerabilities identification.

The methodology is intended to provide a way to better integrate space and cyber operational issues in support of mission analysis and course of action development during the operational planning process.

3. Using the methodology

3.1. Types of contexts

The methodology may be implemented during standing strategic awareness, but is primarily designed to support contingency planning and crisis response planning within existing knowledge development/intelligence and operational planning processes.

3.1.1. During Standing Strategic Awareness

Knowledge centers and intelligence agencies or directorates may apply this methodology as part of their basic intelligence/knowledge development effort within a specific area of interest. Such an effort would particularly focus on the most significant ID dependencies related to the normal use of the various domains in the area of interest, and on the vulnerabilities of Green actors' (for example, 3rd party states) and domain-related actors' (for example: shipping companies or port authorities for the maritime domain) capabilities to potential threats or hazards. Moreover, standing national and multilateral HQs may also develop their ID systems database during this time.

3.1.2. During Operational Planning

When applied within the planning process, the methodology is at the intersection of:

- The intelligence/KD functions, dealing mainly with Red and Green actors' capabilities, as well as related subsystems and operating conditions, through the Preparation of the Operational Environment (POE) process[2];
- Other staff functions, particularly the J5 and J6 functions, in dealing with the Blue capabilities and related subsystems.

The methodology could be implemented for the purpose of analyzing Blue, Green or Red actors' inter-domain dependencies and vulnerabilities. Nevertheless, as currently drafted in this guide, the methodology is focused on Blue and, to a limited degree, Green actors' perspectives.

Figure 3 shows the interaction of the modules with the operational planning process. Figure 4 proposes a detailed flowchart intended to support the implementation of the modules by summarizing the whole methodology at the sub-step level.

[2] As a reminder, generically, a POE process undertaken in support of contingency or crisis response planning, aims a systematic analysis of the operational environment (OE). It combines a systems perspective, through PMESII dimensions, and geospatial perspectives (including land, maritime, air, space and information domains as well as electromagnetic spectrum and weather) of this OE. It uses a four steps – analytical approach:

1- Defining the operational environment;
2- Describing the impact of the operational environment;
3- Evaluation of the actors;
4- Determining adversary courses of action.

3.2. Implications of Using this Guide

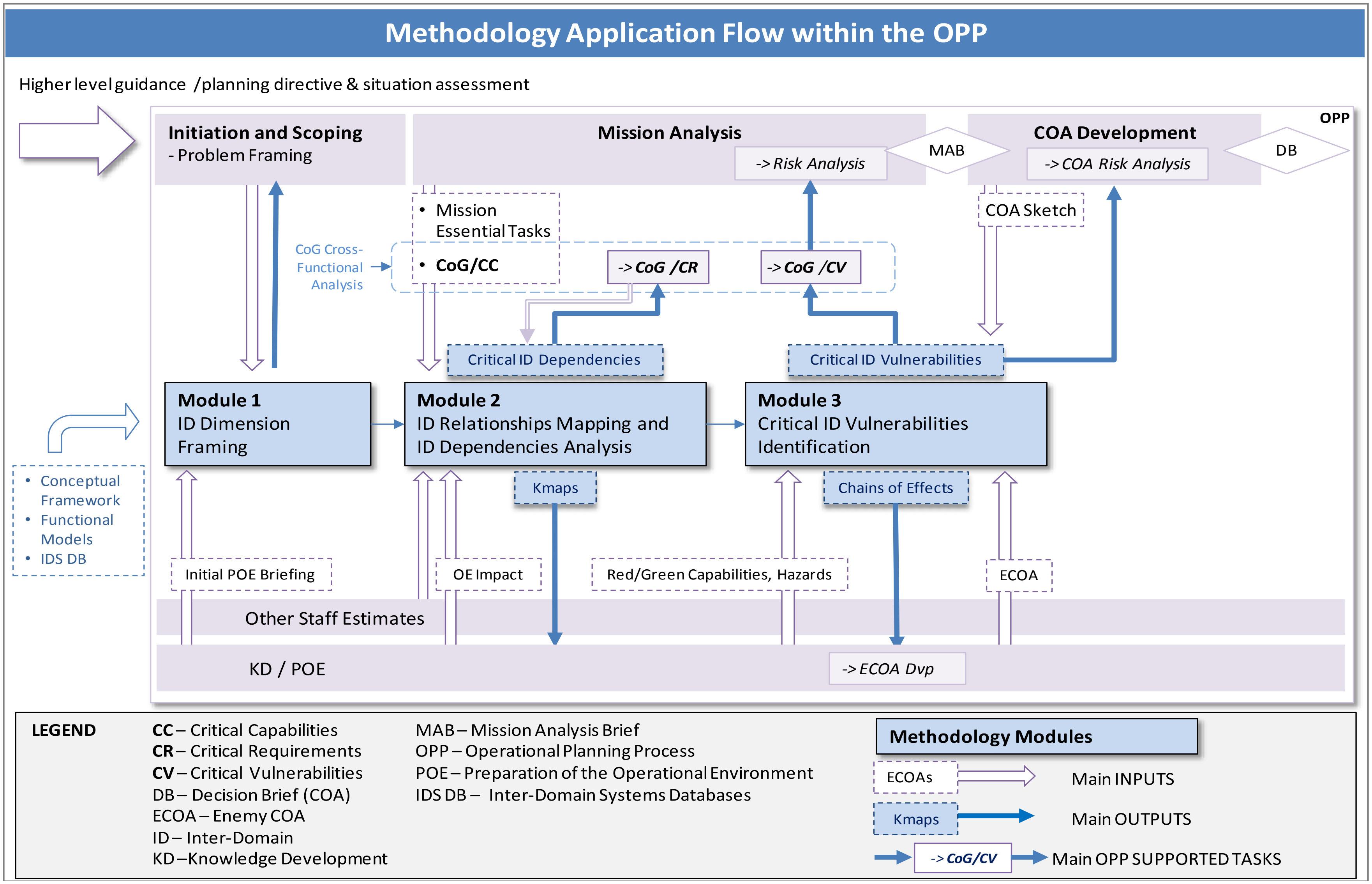
Using this guide in order to identify a coalition's potential vulnerabilities in a given operational context is likely to involve a change in the conduct of staff work, since the methodology proposed is at the intersection of several functions. In the MNE 7 experimental context, the proposed solution was to set up an "**inter-domain working group**" within an operational staff to work together with a joint planning group in order to identify inter-domain issues[3]. It is assumed that the implementation of the guide requires bringing together intelligence and/or knowledge development expertise, planning expertise (J5, J3 and J6) as well as cyber and space expertise, through local liaison or reach back.

[3] Portions of the methodology as described in a version 0.8 of this guide were experimented during a limited objective experiment (LOE) in June 2012.
While participants in the LOE were generally satisfied with the methodology as they applied it and with the results they obtained, the LOE did not enable a complete investigation or "validation" of all of the methodology's steps.
Practitioners composing the experiment audience stated that in their view, the methodology provided:

- A workable way to detect the vulnerabilities of blue forces' inter-domain capabilities;
- Added value and fills a gap in existing analysis and planning processes in terms of ID issues.

However, despite this positive feedback, participants did not consider that the methodology had reached its full maturity and proposed a number of changes, mainly pertaining to its clarification. Recommendations stemming from the LOE are reflected in this version.
Some additional general findings from the LOE are:

- The guide provides a common framework to analyze and work with ID considerations for the different actors involved in the preparation of an operation.
- Cyber and space expertise is essential in order to implement the methodology.



Methodology Application Flow within the OPP

Higher level guidance /planning directive & situation assessment

OPP

Initiation and Scoping
- Problem Framing

Mission Analysis

-> Risk Analysis

MAB

COA Development

-> COA Risk Analysis

DB

- Mission Essential Tasks
- **CoG/CC**

CoG Cross-Functional Analysis

-> CoG /CR

-> CoG /CV

COA Sketch

Critical ID Dependencies

Critical ID Vulnerabilities

Module 1
ID Dimension Framing

Module 2
ID Relationships Mapping and ID Dependencies Analysis

Module 3
Critical ID Vulnerabilities Identification

- Conceptual Framework
- Functional Models
- IDS DB

Kmaps

Chains of Effects

Initial POE Briefing

OE Impact

Red/Green Capabilities, Hazards

ECOA

Other Staff Estimates

KD / POE

-> ECOA Dvp

LEGEND

CC – Critical Capabilities
CR – Critical Requirements
CV – Critical Vulnerabilities
DB – Decision Brief (COA)
ECOA – Enemy COA
ID – Inter-Domain
KD – Knowledge Development

MAB – Mission Analysis Brief
OPP – Operational Planning Process
POE – Preparation of the Operational Environment
IDS DB – Inter-Domain Systems Databases

Methodology Modules

ECOAs → Main INPUTS

Kmaps → Main OUTPUTS

→ ***-> CoG/CV*** → Main OPP SUPPORTED TASKS

Figure 3 – The Methodology Related to an Operational Planning Process

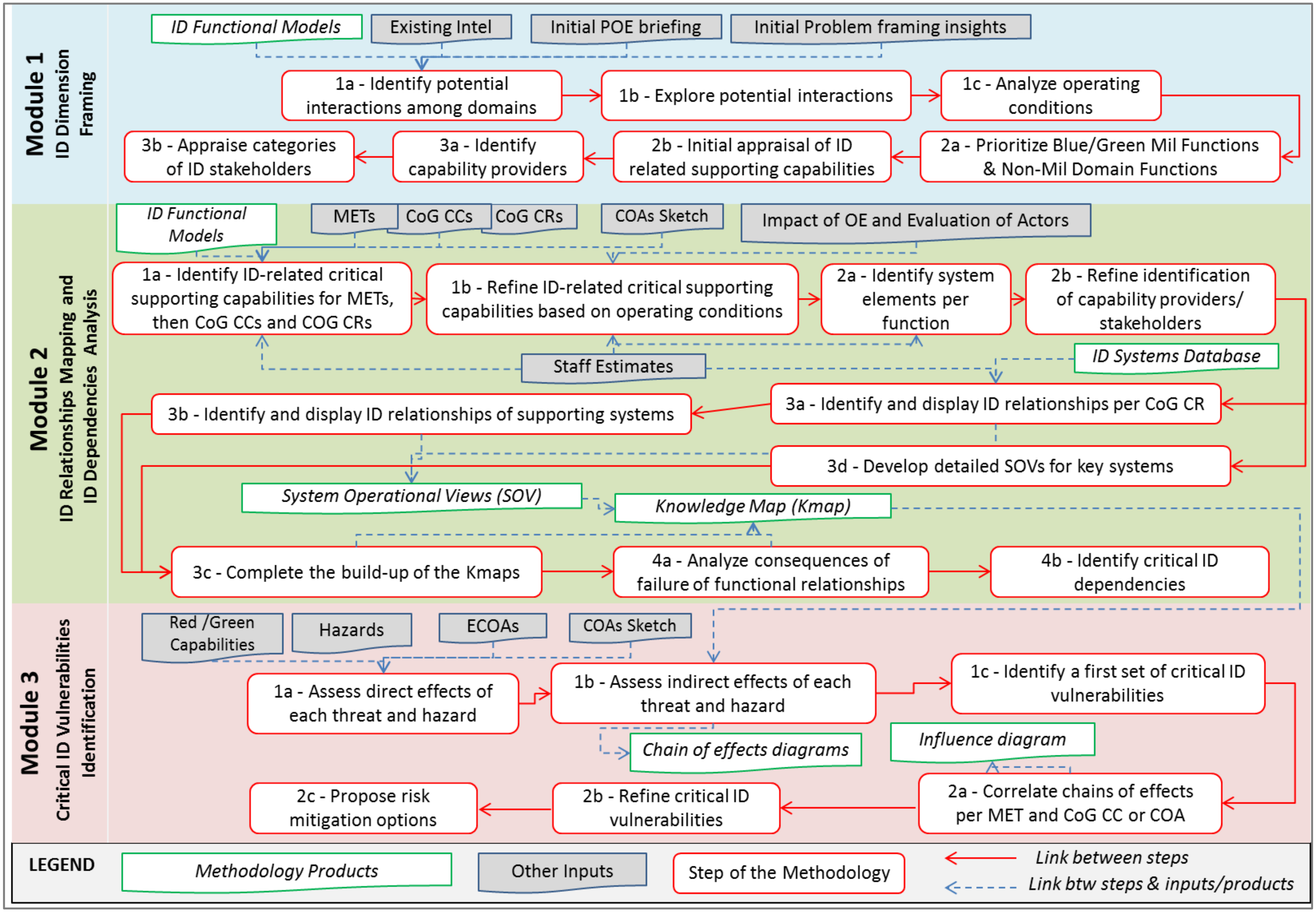

Module 1
ID Dimension Framing
ID Functional Models
Existing Intel
Initial POE briefing
Initial Problem framing insights
1a - Identify potential interactions among domains
1b - Explore potential interactions
1c - Analyze operating conditions
3b - Appraise categories of ID stakeholders
3a - Identify capability providers
2b - Initial appraisal of ID related supporting capabilities
2a - Prioritize Blue/Green Mil Functions & Non-Mil Domain Functions
Module 2
ID Relationships Mapping and ID Dependencies Analysis
ID Functional Models
METs
CoG CCs
CoG CRs
COAs Sketch
Impact of OE and Evaluation of Actors
1a - Identify ID-related critical supporting capabilities for METs, then CoG CCs and COG CRs
1b - Refine ID-related critical supporting capabilities based on operating conditions
2a - Identify system elements per function
2b - Refine identification of capability providers/ stakeholders
Staff Estimates
ID Systems Database
3b - Identify and display ID relationships of supporting systems
3a - Identify and display ID relationships per CoG CR
3d - Develop detailed SOVs for key systems
System Operational Views (SOV)
Knowledge Map (Kmap)
3c - Complete the build-up of the Kmaps
4a - Analyze consequences of failure of functional relationships
4b - Identify critical ID dependencies
Module 3
Critical ID Vulnerabilities Identification
Red /Green Capabilities
Hazards
ECOAs
COAs Sketch
1a - Assess direct effects of each threat and hazard
1b - Assess indirect effects of each threat and hazard
1c - Identify a first set of critical ID vulnerabilities
Chain of effects diagrams
Influence diagram
2c - Propose risk mitigation options
2b - Refine critical ID vulnerabilities
2a - Correlate chains of effects per MET and CoG CC or COA
LEGEND
Methodology Products
Other Inputs
Step of the Methodology
Link between steps
Link btw steps & inputs/products

Figure 4 - Detailed Flowchart of the Methodology

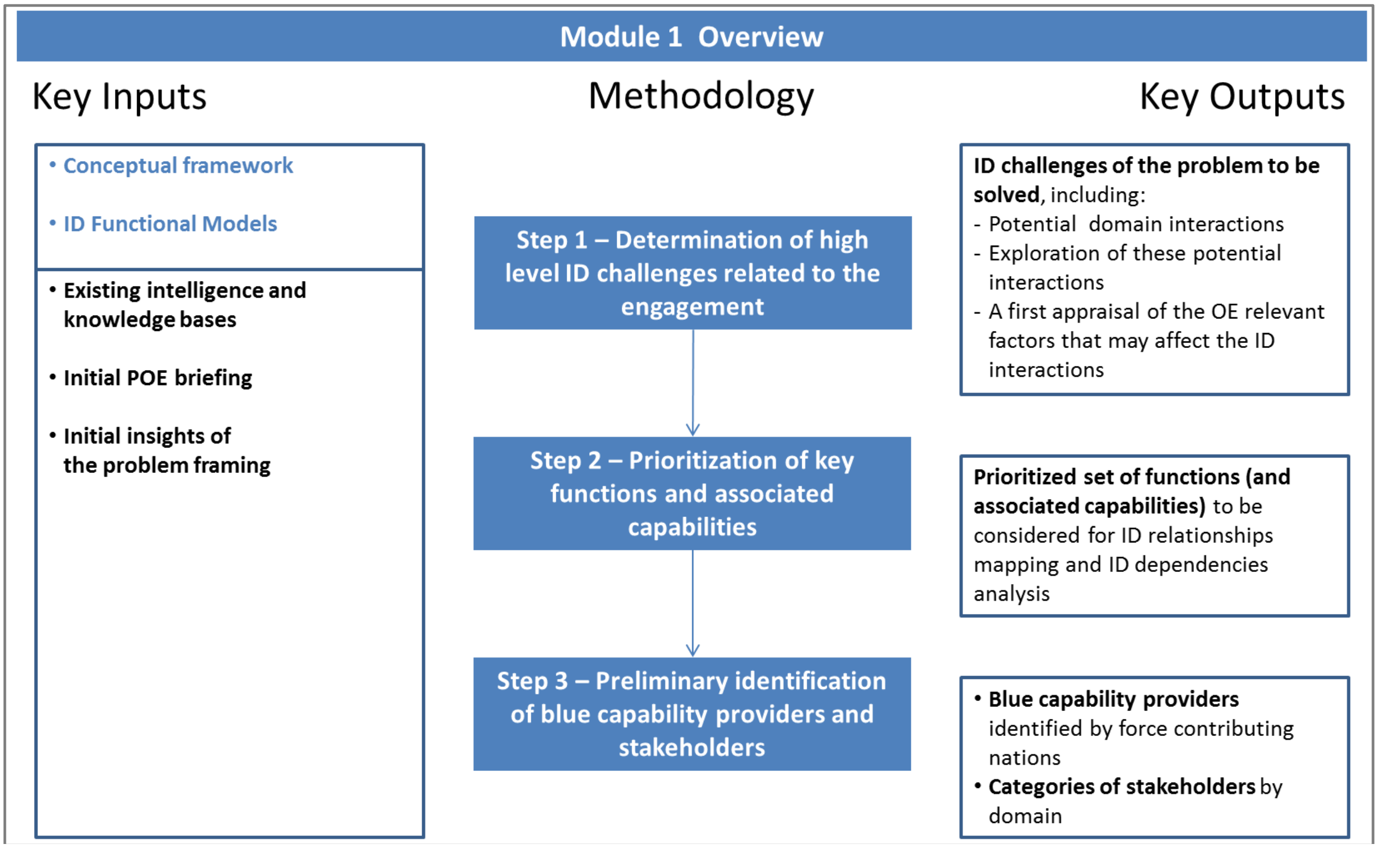
Intentionally Blank

Module 1: Framing the Inter-Domain Dimension of the Engagement

The objective of this module is to determine the inter-domain dimension of the Commander's perspective of the engagement in order to orient subsequent modeling and analysis efforts. Based on the nature of the engagement, the actors involved, their strategies and their capabilities, in this module, the focus is on the determination of the inter-domain challenges, on the prioritization of functions and capabilities and on the identification of the main stakeholders.

This module offers a complementary perspective to the problem framing of the engagement performed by the Commander and his or her staff. It should therefore be integrated into the "problem framing", as part of the initiation and scoping step of the planning process[4].

The figure below depicts the main inputs of this module, the main steps involved, and the expected outputs.



Module 1 Overview

Key Inputs

- Conceptual framework
- ID Functional Models

- **Existing intelligence and knowledge bases**
- **Initial POE briefing**
- **Initial insights of the problem framing**

Methodology

Step 1 – Determination of high level ID challenges related to the engagement

Step 2 – Prioritization of key functions and associated capabilities

Step 3 – Preliminary identification of blue capability providers and stakeholders

Key Outputs

ID challenges of the problem to be solved, including:
- Potential domain interactions
- Exploration of these potential interactions
- A first appraisal of the OE relevant factors that may affect the ID interactions

Prioritized set of functions (and associated capabilities) to be considered for ID relationships mapping and ID dependencies analysis

- **Blue capability providers** identified by force contributing nations
- **Categories of stakeholders** by domain

Figure 5: Module 1 Overview

[4] In the NATO COPD, the equivalent of initiation and scoping takes place with the Operational Orientation phase.

1. Inputs to Module 1

The following inputs are necessary to implement this module:

1. The ID functional models[5] described in appendix B that would have been developed in advance;
2. The key terms described in Appendix D, which provide an intellectual framework to think about ID issues[6];
3. Existing intelligence and knowledge bases and if available:
   - The main characteristics of the operational environment, including PMESII analysis;
   - Initial preparation of the operational environment materials;
   - Existing ID-related analysis that could have been developed during standing strategic awareness.
4. First insights from the problem framing, including:
   - A first sketch of the Red (and potentially Green) actor's design or operational approach (outlining its aims, objectives and strategy) and capabilities;
   - An overall analysis of the systemic nature of the crisis.

2. Module 1 Method

Module 1 is composed of three steps, which have been further divided into a number of proposed sub-steps. Framing the ID dimension of the engagement may be undertaken by applying the steps described here.

2.1 Step 1: Determination of the High Level ID Challenges Related to the Engagement

The determination of the ID challenges seeks to identify whether there are any inter-domain problems in the engagement space. The ID challenges are derived from the initial analysis of the potential effect of Red and Green capabilities and operating conditions on Blue, Green and non-military domain users' capabilities.

This analysis may be conducted in the following manner:

a. **Identify the potential interactions among domains.** This is done by undertaking an initial identification of the domains and related military and civilian activities that could be affected by Red and/or Green actors' offensive and defensive capabilities, given the emerging characteristics of the engagement and the mission given to the commander. It leads to the formulation of open questions.

[5] These provide an idea of the types of capabilities and systems required for each function and aim to facilitate the identification of the potential systems and assets to be considered.

[6] For more detail on this conceptual framework please refer to the MNE7 Outcome 4 Conceptual and Pre-Doctrinal Paper: Understanding Inter-Domain Dependencies and Vulnerabilities, dated 31 January 2013.

b. **Explore these potential interactions**. This is done by analyzing the ways the Red actor could seek to use these capabilities to affect or exploit the considered military and civilian activities or capabilities in one or more domains as identified in sub-step a. It leads to the formulation of hypotheses and assumptions regarding the potential effects of these capabilities. These hypotheses and assumptions constitute a first set of ID challenges.

c. **Analyze the operating conditions** and the way that they could affect the Blue, Green, Red and non-military capabilities and activities in the engagement space in order to bring to light potential inter-domain implications. This first appraisal takes into account the nature of the PMESII and geospatial dimensions of the operational environment and the timeframe of the engagement. It leads to the formulation of key conditions and potentially to additional ID challenges.

This analysis will be supported by the development of one or several cognitive diagram(s) and a supporting narrative distinguishing and explaining these ID challenges. These products will constitute the output of this first step of module 1.

***Example**: Within the context of the problem framing for an anti-piracy engagement, the initial POE points out that pirates are probably allied with hackers and display the will to disrupt anti-piracy operations to protect their activities.*

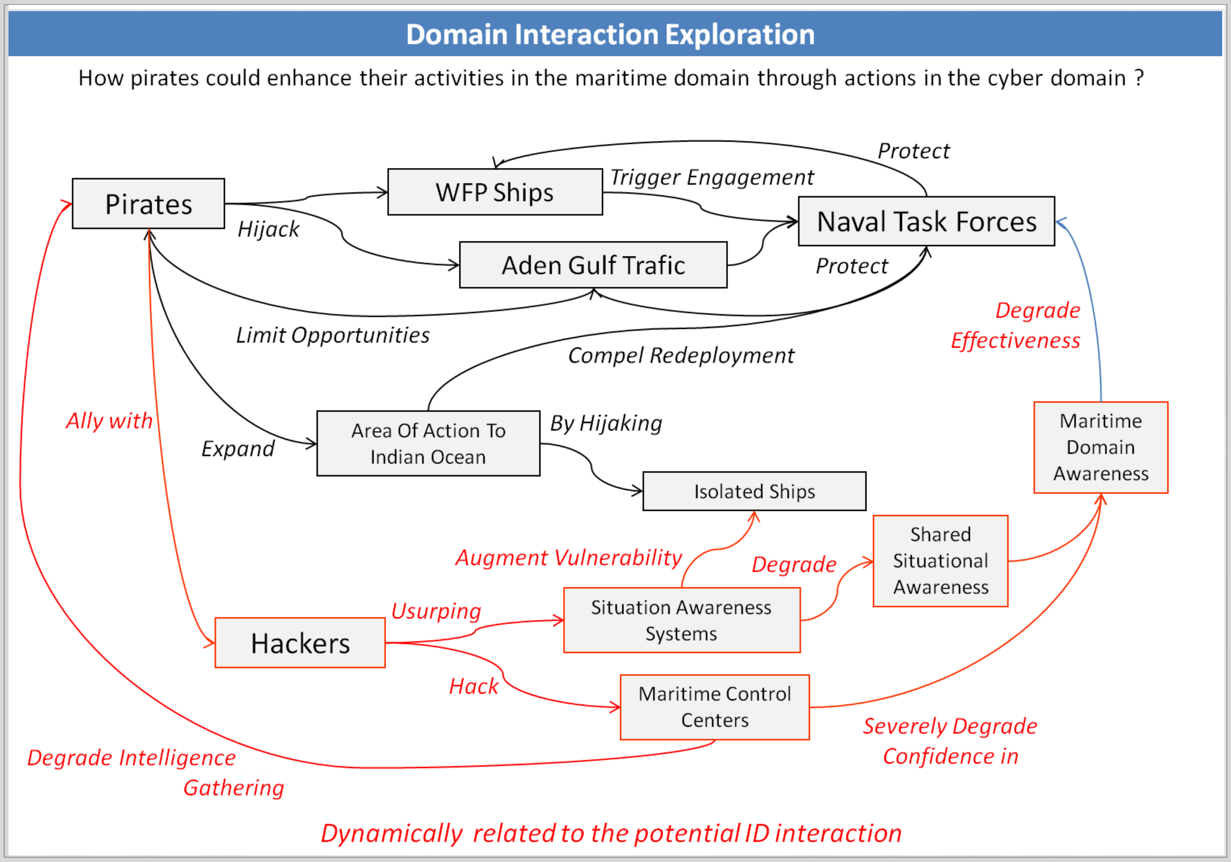
a - The initial identification of potential interactions among domains leads to the formulation of open questions: How could pirates enhance their activities in the maritime domain through actions in the cyber domain? What are the risks for the action of the international naval forces?

b - The exploration of these potential interactions is depicted in the cognitive diagram below and would lead to the formulation of hypotheses such as:

If pirates form an alliance with hackers, then they will have the will, the intent and the capability:

- to hack maritime control centers and thereby to degrade confidence in maritime domain awareness (1st ID challenge);

- to usurp situational awareness systems which would increase the vulnerability of isolated ships and degrade situational awareness (2nd ID challenge).



Domain Interaction Exploration

How pirates could enhance their activities in the maritime domain through actions in the cyber domain ?

Dynamically related to the potential ID interaction

Figure 6: Illustrative Cognitive Diagram of the Analysis Exploration of a potential ID Interaction.

c - Furthermore, the size and the political and geospatial characteristics of the maritime JOA, with limited basing options, entail a reliance on air long endurance assets for surveillance.

2.2 Step 2 - Prioritization of the Key Functions and Associated Capabilities

The Commander and his staff should review the ID challenges resulting from the application of step 1 and identify which military functions and non-military domain functions could potentially be affected by each one. Following this review, the Commander and his or her staff would:

a. **Select and prioritize the Blue and Green military functions, as well as non-military domain functions, in order to focus the effort of the subsequent modeling of the ID System**[7]. When possible, the staff should formulate the main effect that the adversary could seek to obtain for each prioritized function based on the ID challenges[8].

[7] While it may assumed that C2 and Intelligence, primarily supported by space and cyber capabilities will often be among the priorities, the consideration of other functions will depend on this analysis.

[8] For example, if C2 is identified as an important military function, the staff could qualify the effect the adversary would try to obtain by stating "degradation of C2".

b. **Provide, to the extent possible, an initial appraisal of the ID-related supporting capabilities** required for each of the prioritized military functions and non-military domain functions, based on an initial understanding of the engagement[9]. In many instances, the considered capabilities will be necessary for multiple functions. This appraisal should draw on the ID functional models, which provide an idea of the types of capabilities and systems required for each function and aim to facilitate the identification of the systems and assets to be considered.

The result of this step would be a list of prioritized functions (military functions and non-military domain functions) and the main associated capabilities[10].

Example*: In the example of an anti-piracy engagement, the challenges that hackers could pose for situational awareness systems and maritime control centers entail placing a priority on analyzing the international naval force's C2 and Intelligence military functions, and the "maritime access and operations" non-military domain function in the area of interest. The main capabilities to be considered would be:*

- *The civil-military information management capabilities (for the C2 and Intelligence military functions);*
- *The primary reliance on air remote sensing capabilities (for the Intelligence function), which would thereby limit the need to consider all the ID supporting elements for space ISR.*

2.3 Step 3 – Preliminary Identification of Blue Capability Providers and Stakeholders

This step focuses on the preliminary identification of the capability-providers and stakeholders by function (military function and non-military domain function) and/or capability to complete the framing of the inter-domain dimension of a given engagement. The purpose of this step is to guide subsequent analysis and knowledge collection efforts in module 2. It is comprised of two sub-steps:

a. **Identify the specific capability providers** – particularly space and cyber ones – **for each of the prioritized Blue military functions**[11]. Each force contributing nation or participating nation would be expected to know who its capability providers are. While they may not be able to share the specifics of this information with partners, each nation will need to go through this step in order to prepare for reach-back or coordination in later steps of the methodology. Capability-providers may be controlled by Blue actors or be external actors with means that the force relies on.

[9] It is assumed that a rough identification of the primary capabilities would be done as part of the existing planning process, by the various staff functions.

[10] The number of functions to be studied will depend on the time available.

[11] These capability providers will provide the expertise needed to complete module 2. This may draw from other staff estimates (such as J6 and J2) if they already exist or could support their development by helping to focus them.

b. **Establish a first appraisal of the broad categories of stakeholders based on the ID challenges.** For each ID challenge, the analysis would present a preliminary identification of the actors who could be affected by a given ID challenge. The purpose of this sub-step is to guide the specific analysis of stakeholders in module 2.

Example*: In the example of an anti-piracy engagement, one hypothesis related to pirates acting through cyber hacking to enhance their maritime activities; therefore, organizations and centers involved in the management of local maritime transit and the main shipping companies would be among the main categories of stakeholders.*

3. Outputs of Module 1

The outputs of this phase are:

<u>Step 1</u>: ID challenges to be addressed including:

- Hypotheses and assumptions relating to potential interactions among domainsl
- A first appraisal of the operating conditions that may affect interactions among domains.

<u>Step 2</u>: Prioritized set of functions (military functions and non-military domain functions), and to the extent possible, required supporting capabilities to be considered to map the ID relationships and analyze the ID dependencies in module 2.

<u>Step 3</u>: Preliminary list of capability providers and stakeholders.

Similarly to other efforts contributing to the problem framing, the framing of the ID dimension of the engagement is mainly supported by written narratives and cognitive diagrams.

* * *

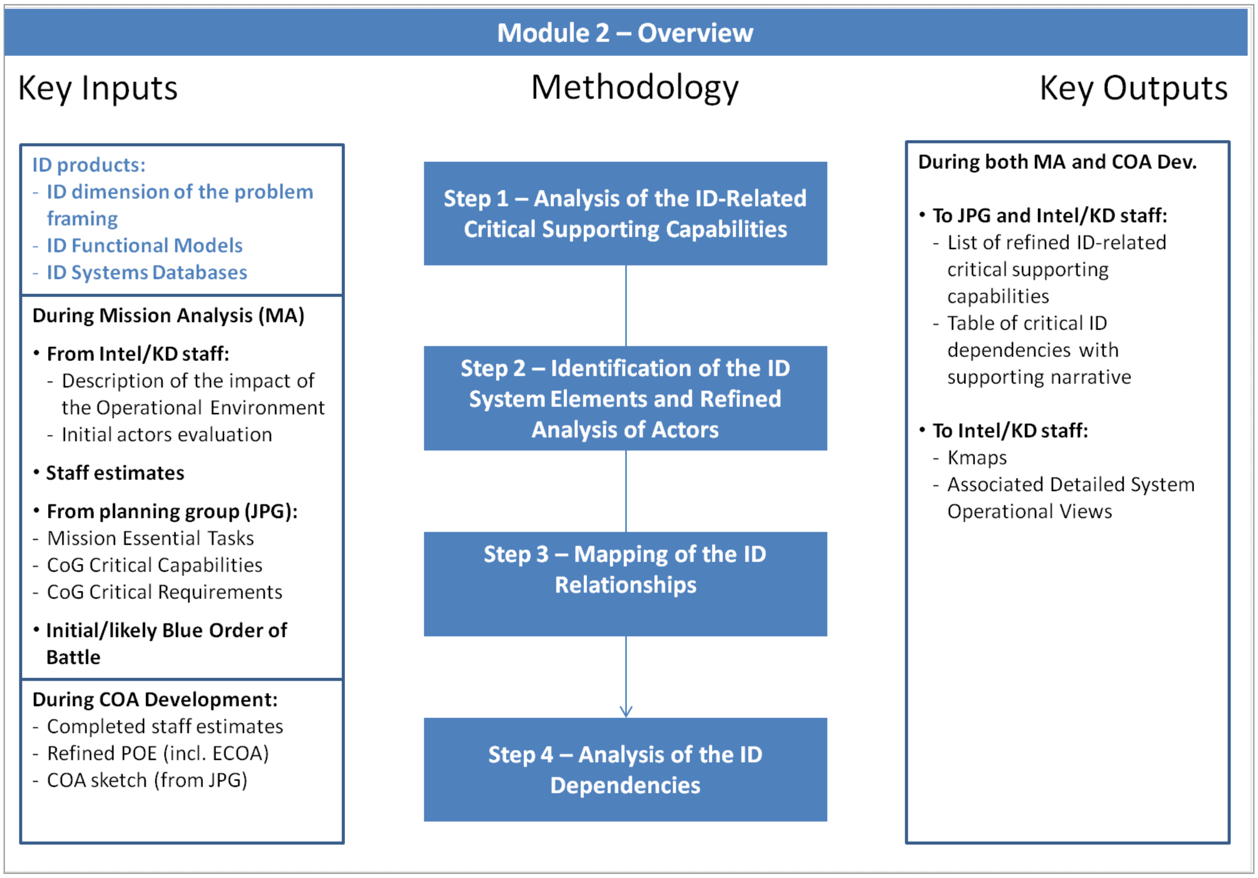
Module 2: ID Relationships Mapping and ID Dependencies Analysis

The aim of this module is **to identify the key ID relationships between the elements of the ID System and the critical inter-domain dependencies, in order to support:**

- **The center of gravity analysis during mission analysis;**
- **The development of courses of action.**

As described here, this module is primarily intended to improve understanding of relationships and dependencies from a Blue perspective, based on the prioritized functions identified in the previous module. It can also be applied to understanding the Green perspective and non-military domain functions as defined in module 1[12].

The figure below depicts the key inputs of module 2, its methodology and its expected outputs.



Module 2 – Overview

Key Inputs

ID products:
- ID dimension of the problem framing
- ID Functional Models
- ID Systems Databases

During Mission Analysis (MA)
- **From Intel/KD staff:**
  - Description of the impact of the Operational Environment
  - Initial actors evaluation
- **Staff estimates**
- **From planning group (JPG):**
  - Mission Essential Tasks
  - CoG Critical Capabilities
  - CoG Critical Requirements
- **Initial/likely Blue Order of Battle**

During COA Development:
- Completed staff estimates
- Refined POE (incl. ECOA)
- COA sketch (from JPG)

Methodology

Step 1 – Analysis of the ID-Related Critical Supporting Capabilities

Step 2 – Identification of the ID System Elements and Refined Analysis of Actors

Step 3 – Mapping of the ID Relationships

Step 4 – Analysis of the ID Dependencies

Key Outputs

During both MA and COA Dev.
- **To JPG and Intel/KD staff:**
  - List of refined ID-related critical supporting capabilities
  - Table of critical ID dependencies with supporting narrative
- **To Intel/KD staff:**
  - Kmaps
  - Associated Detailed System Operational Views

Figure 7: Module 2 Overview

[12] As stated previously, it could be adapted in order to identify an adversary's critical ID dependencies.

1. Inputs to Module 2

During mission analysis, the following inputs are necessary to implement this module:

- The ID dimension of the engagement within problem framing (output of module 1), which helps to focus the mapping;
- The ID functional models (described in appendix B);
- The key terms (described in Appendix D)[13];
- The database describing the inter-domain relationships among systems that could potentially be used, including the systems operational views (described in appendix C);
- Intelligence/KD products:
  - The description of the impact of the operational environment (POE step 2);
  - Initial insights regarding the evaluation of actors (POE step 3);
- The staff estimates;
- The Mission Essential Tasks[14] (including space and cyber supporting tasks) and the CoG critical capabilities and initial critical requirements developed by the joint planning group;
- The initial or likely Order of Battle.

When this module is refined **during COA development**, it is based on

- The refined and completed staff estimates and POE, including Enemy COAs, and
- The operational design refined at the end of the mission analysis and the initial sketch of each COA developed by the joint planning group.

2. Module 2 Method

This module encompasses:

- The analysis of the critical ID-related supporting capabilities in support of the CoG analysis (step 1);
- The identification of the elements of the ID System (step 2);
- The mapping of the relevant elements of the ID System, and their various relationships (step 3);
- The analysis of the ID dependencies (step 4).

2.1 Step 1: Analysis of the Critical ID-related Supporting Capabilities

This step aims to help the staff to understand which supporting capabilities (primarily space and cyber capabilities) are the most important for the mission, and among them, which are the most relevant given the operating conditions. This is done by further elaborating on the initial list of capabilities identified in module 1.

[13] For more detail on this conceptual framework please refer to the MNE7 Outcome 4 Conceptual and Pre-Doctrinal Paper: Understanding Inter-Domain Dependencies and Vulnerabilities, dated 31 January 2013.

[14] Note that NATO uses the term "Mission Essential Action" in the COPD.

When analyzing the Blue capabilities, this complementary analysis should be executed as an integral part of the mission analysis and more specifically as part of the analysis of the Mission Essential Tasks (METs) and the Center of Gravity (CoG) led by the joint planning group. The objective of this step is to identify more specifically which space and cyber capabilities are needed to support the first expression of CoG critical requirements[15]. This will then be used to focus the analysis of the critical ID dependencies.

The figure below portrays how the methodology complements center of gravity analysis by providing an inter-domain perspective. As the figure shows, although this work begins during this step, it continues in module 3.

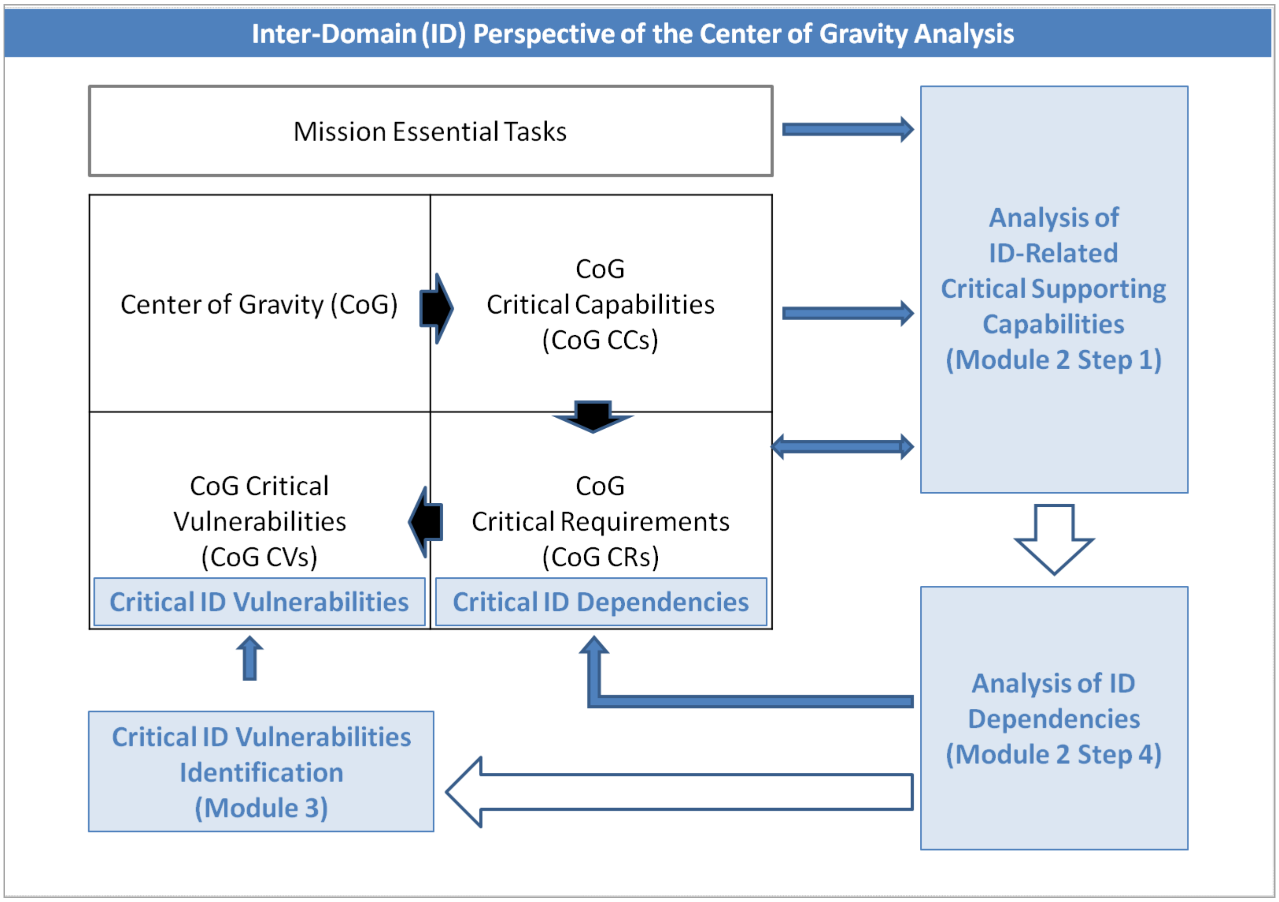

Inter-Domain (ID) Perspective of the Center of Gravity Analysis
Mission Essential Tasks
Center of Gravity (CoG)
CoG Critical Capabilities (CoG CCs)
CoG Critical Vulnerabilities (CoG CVs)
CoG Critical Requirements (CoG CRs)
Critical ID Vulnerabilities
Critical ID Dependencies
Analysis of ID-Related Critical Supporting Capabilities (Module 2 Step 1)
Analysis of ID Dependencies (Module 2 Step 4)
Critical ID Vulnerabilities Identification (Module 3)

Figure 8 - ID Perspective of the Center of Gravity Analysis

This step is divided into two sub-steps which may be executed in parallel or sequentially:

a. **Determine the critical ID-related supporting capabilities** (primarily space and cyber). This is done in an iterative manner, based on the mission essential tasks and the Center of Gravity analysis. Based on the METs and the center of gravity critical capabilities (CoG CC) given by the

[15] This approach should help the staff to conduct a cross-functional analysis of the CoG (in the sense that it should not look at each military function in a compartmentalized manner).

joint planning group, a first list of critical ID-related supporting capabilities is determined. These critical ID-related supporting capabilities contribute to the identification of the CoG critical requirements (CoG CR)[16]. Finally, the list of critical ID-related supporting capabilities is again refined and/or complemented with new elements based on the CoG CR.

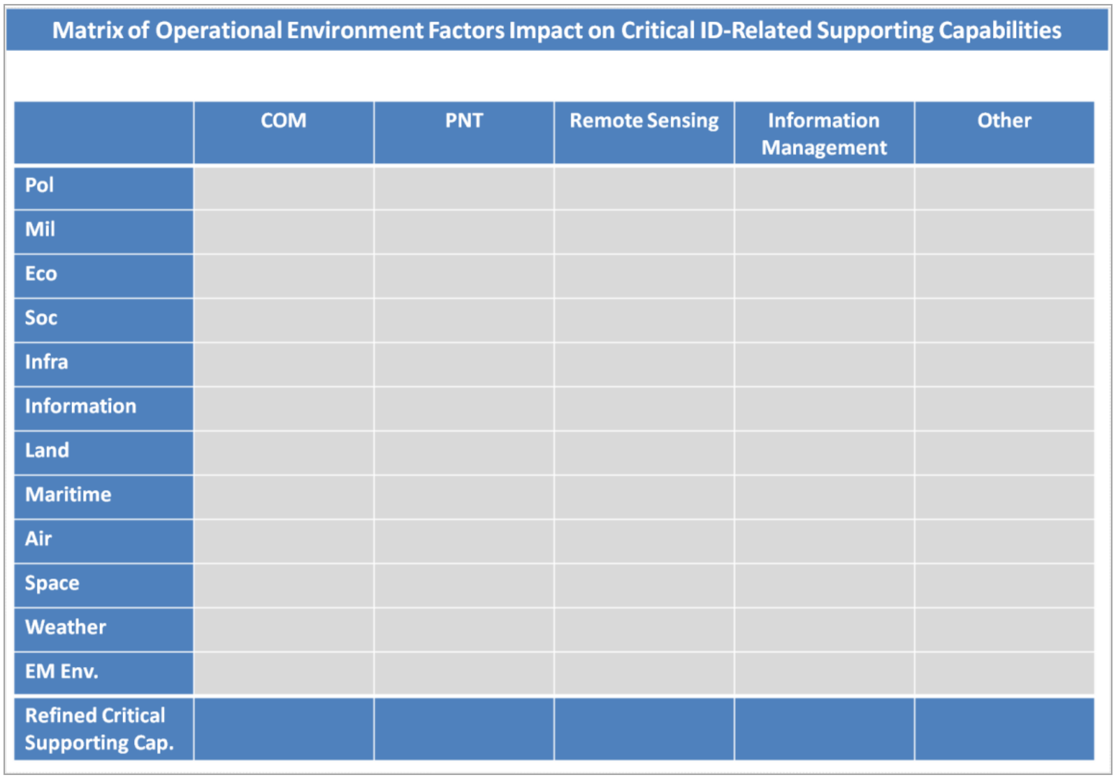
b. **Further refine the analysis of these critical ID-related supporting capabilities based on the operating conditions** provided by the staff estimates and the evaluation of the impact of the operational environment (POE step 2) and evaluation of actors (POE step 3) developed by Intelligence and KD staffs.

This refinement is a prolongation of the initial analysis undertaken in module 1 when framing the ID dimension of the engagement. The list of critical ID-related supporting capabilities is refined based on:

- The initial results of the evaluation of the land, air, maritime, space and information domains of the operational environment as well as relevant PMESII dimensions (step 2 of POE) and of the evaluation of the adversary capabilities;
- Elements regarding the Blue forces' communications and information management, drawn from the analysis done in staff estimates:
  - The initial structure for each military function (i.e. C2 or intelligence structure);
  - The information flow requirements as developed by the J3 and J2 (e.g. the RFI flow for the intelligence function);
  - The communications systems options and associated constraints, as provided by the J6 estimate.

This analysis of the implications of the operating conditions may be conducted by developing a matrix as represented in the figure below displaying on one hand the conclusions of the POE for each dimension of the operational environment and on the other hand the ID-related supporting capabilities identified as potentially critical for the MET and CoG CC and CR.

[16] Often, these MET and CoG CC remain very broad in scope and not specific enough to focus the analysis of dependencies. For example, an MET such as "establish situational awareness over the JOA" may potentially encompass all systems considered in the intelligence function. Besides, critical requirements, as traditionally formulated, deal primarily with the most obvious operational assets (command nodes, combat assets, etc.)



Matrix of Operational Environment Factors Impact on Critical ID-Related Supporting Capabilities

	COM	PNT	Remote Sensing	Information Management	Other
Pol					
Mil					
Eco					
Soc					
Infra					
Information					
Land					
Maritime					
Air					
Space					
Weather					
EM Env.					
Refined Critical Supporting Cap.					

Figure 9 - Operational Environment Impact Matrix

The output of this step is a list of refined critical ID-related supporting capabilities relative to the critical requirements already identified by the joint planning group.

***Example**: For MET "Conduct area interdiction operations in the JOA", the COG analysis, complemented by the analysis of the critical ID-related supporting capabilities could arrive at the following results:*

- *Intelligence CC: the ability to provide timely target intelligence;*

○ *CR: 1-UAS X & Y, 2-Recce system Z*

○ *Critical ID-related supporting capability: given the characteristics of the JOA, reliance on BLOS provided by SATCOM systems*

- *Command and control CC: the ability to command and control air interdiction operations*

○ *CR: JFHQ and JFACC command nodes*

○ *Critical ID-related supporting capability: secured intra-theater BLOS capability between JFHQ and JFACC and reach back to supporting rear HQs*

- *Fires CC: the ability to strike on adversary C2 and transportation target sets*

○ *CR: Air interdiction – related systems: air strike units and sea-launched cruise missiles*

○ *Critical ID-related supporting capability: PNT capability for cruise missiles and other PGM guidance.*

This analysis of the critical ID-related supporting capabilities should be refined during the COA development. It would lead to a tailored list of refined of critical supporting capabilities for each COA developed by the joint planning group.

2.2 Step 2: Identification of ID System Elements and Refinement of Actor Analysis

The purpose of this step is to list the systems and assets and associated capability providers and stakeholders. This information will be used in the subsequent steps in the analysis of the ID relationships and dependencies.

This step involves a number of sub-steps:

a. **Identify the ID System elements**: For each selected and prioritized military function and considered non-military domain function, list the systems or assets needed for the primary and supporting capabilities. This identification of the systems and assets should be supported by the ID functional models.

The known systems and assets are drawn from the Blue force likely or initial order of battle and supplemented by staff estimates, notably the J6 and J2 estimates. For Green and non-military domain-related assets, this information is provided by the PMESII analysis and other sources.

b. **Refine the analysis of capability providers and stakeholders** based on the identified ID System elements.

The refined analysis of the capability providers (for the Blue capabilities) is done by identifying which entity provides and controls a system (military or civilian, public or private) and where to get additional information if needed. While this analysis clearly remains a national responsibility, each force contributing nation or participating organization would be expected to share the relevant information regarding its capability providers.

Building on the categories of stakeholders identified in module 1 and taking into account the ID System elements identified in the previous sub-step, specific stakeholders should be identified. They should be categorized in terms of level of interest and influence in the area for the considered activities, and their expected attitude regarding the Red, Green and Blue actors.

> *For example in the maritime domain, the relevant actors would be:*
> *- The port authorities of country X: Their interest in maintaining shipping activities despite the crisis, is the same as that of Green state A and they are likely to remain neutral - The port's main internet provider: It is strictly controlled by the country X government;*
> *- The main shipping companies: Most of the shipping transiting in the considered area relies on companies A, B and C of country Z, an ally of the Red actor;*
> *- The providers of SATCOM services used by ships: mainly Western companies.*

The result of this analysis is a tree diagram or a table listing available systems or assets for each relevant military function and for the considered non-military domain functions, as well as a refined list of stakeholders.

2.3 Step 3: Mapping of ID Relationships

The objective of this step is to identify and map the key relationships in the ID System. To do so, analysts should map, from a functional perspective[17], the inter-domain relationships between the systems that make up the CoG critical requirements (CoG CR) as given by the joint planning group and the ID System elements identified in step 2. During COA development, this mapping should be updated as required for each envisioned COA.

The main product resulting from the mapping of ID relationships is a set of "knowledge maps" (called Kmaps). Depending on the circumstances, **a Kmap may be developed for a given military function, non-military domain function, cross-functional CoG critical capability or for a specific ID challenge,** as identified in module 1. The number of Kmaps developed will depend on the nature of the ID challenges and the time available. These Kmaps should be interlinked to determine the cross-functional systems[18].

The degree to which the sub-steps described below can be applied will depend on the time, the data, the staff and technical expertise available. When a limited amount of time and data are available, the mapping and subsequent analysis will primarily consider each system as one entity and will focus on their functional[19] relationships without delving into their own segments or elements of this system. When there is more data and time available, the mapping and analysis should delve further into the functional and physical relationships between system elements, thereby providing a greater degree of granularity in the dependencies analysis.

The Elements of a Kmap

A Kmap is an annotated network analysis diagram, such as those developed by intelligence or KD systems analysts to analyze the operational environment. It aims to outline, for a given function, the functional inter-domain relationships between the critical requirements and supporting systems. In order to keep the diagram manageable and exploitable, the Kmap should represent each system (such as a SATCOM system for example) as one entity, without detailing its various components. A Kmap is neither a technical nor a geospatial diagram of the structural relationships.

A Kmap represents the aggregation of "system operational views" (SOV). A system operational view is, for a given system, the elementary network of its ID functional relationships and supporting systems.

[17] In the sense of the military functions and non-military domain functions.

[18] This can be done manually, or ideally, with the help of a tool. *For example, the analyst should be able to superimpose or switch from the C2 Kmap to the intelligence Kmap when he or she works on the dependencies stemming from a given CWAN critical for both functions.*

[19] The term "functional" here is used in the generic sense (not related to the military functions or the non-military domain functions)

The Kmap is intended to be enriched during the dependencies analysis and should enable a visualization of the relationships and dependencies as qualified in step 4 of module 2.

Systems Operational Views and Kmaps should include the following elements:

- A symbology outlining:
  - The ID System elements (systems, assets) providing the capabilities, distinguished by domain: space, air, maritime, land and cyber[20];
  - The functional relationships;
  - The enabling relationships;
  - The enhancing relationships;
  - The critical ID dependencies;
- Text boxes outlining relevant information regarding the considered element, relationships and dependencies.

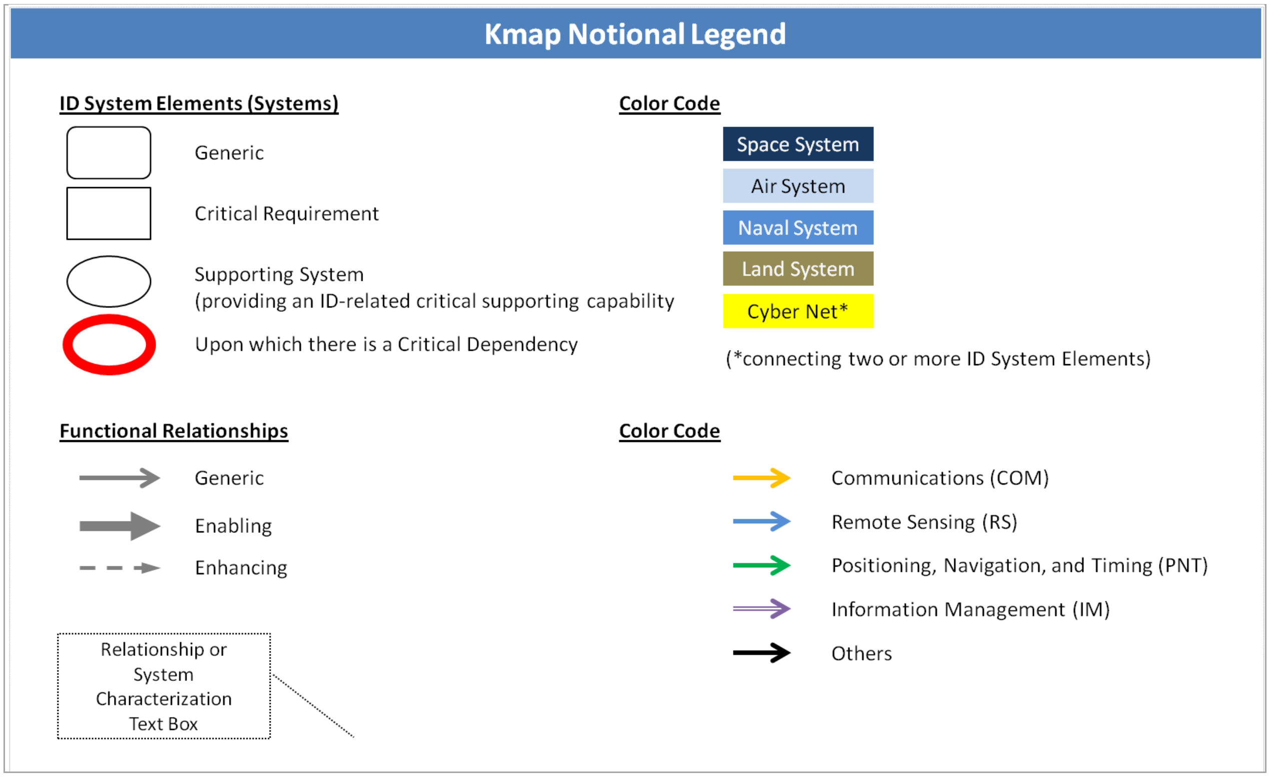

Kmap Notional Legend
ID System Elements (Systems)
Generic
Critical Requirement
Supporting System
(providing an ID-related critical supporting capability
Upon which there is a Critical Dependency
Color Code
Space System
Air System
Naval System
Land System
Cyber Net*
(*connecting two or more ID System Elements)
Functional Relationships
Generic
Enabling
Enhancing
Color Code
Communications (COM)
Remote Sensing (RS)
Positioning, Navigation, and Timing (PNT)
Information Management (IM)
Others
Relationship or System Characterization Text Box

Figure 10 - Notional legend of a Knowledge Map

A Kmap (example in Figure 12) **should ideally be complemented and supported by detailed SOVs** (example in Figure 11), which aim to outline the functional and physical ID relationships among the elements of some key systems and between these elements and their supporting systems (for example, the space, ground and user segments of the SATCOM system). The detailed SOVs offer a more granular view of the ID relationships depicted in the Kmap.

[20] Many elements belong to both one of the physical domain and the cyber domain. By convention, cyber elements represented in the Kmap include the cyber networks connecting two or more elements, the other elements are representing according to their main physical domain. For example, a SATCOM will be represented as a space system. Moreover, the cyber element within an element, such as local area network within a HQ will not be represented.

This step can be divided into four sub-steps:

- Identify ID relationships and supporting systems related to the critical requirements (enrich the ID systems database if it exists and develop the system operational views);
- Develop the SOVs for the supporting systems themselves;
- Complete the build-up of the Kmap by connecting these system operational views;
- Concurrently, when possible and necessary, develop detailed system operational views.

a. **Identify and display the ID relationships and the supporting systems for each system or asset that constitutes a critical requirement.** *For example, UAS X requires SATCOM Y for its data dissemination and GPS for PNT*[21]. The result of this sub-step is an SOV for each critical requirement.

ID relationships and related supporting systems are ideally drawn from:

- The list of the ID system elements identified in the previous step;
- The information in the ID systems database and pre-developed systems operational views (see appendix C regarding recommendations for tools) which provide generic ID relationships for a given system.

One way to capture all the identified relationships and related supporting systems is to add them into the ID systems database.

The generic ID relationships and related systems **should be refined and adjusted,** as required, **according to the context of the engagement,** by taking into account:

- **The characteristics of critical ID-related supporting capabilities** which may emphasize the use of specific systems and lead to discarding others given the operational environment and other mission related-factors. This is directly drawn from the analysis of the critical ID-related supporting capabilities performed in step 1. *For example, the size of JOA implies a reliance on BLOS communication, emphasizing the need to map SATCOM systems rather than other LOS systems*.
- **The availability of the various supporting systems.** *For example, a civilian SATCOM system supporting a coalition ISR system may not be available at the time of the engagement*.

This refinement may lead to the removal of some systems and relationships.

The SOVs are then developed on a Kmap template for each prioritized military function and non-military domain function or for the selected CoG critical capability.

[21] Note that information-sharing limitations between force contributing nations or the fact that troop contributing nations have not yet committed their means, may lead to a lack of data. If the data are still lacking, a generic functional mapping may be undertaken *(i.e. the required MALE UAS will need Ku-Band SATCOM to relay its collected data).*
The methodology proposes drawing from a database and associated system operational views to accelerate the process. For example, this sub-step could be conducted by exploiting ID systems databases which could allow the automatic graphical depiction of the ID relationships and elements supporting each system. Having a tool to enable the automatic extraction of data and their transfer into the Kmaps would be an essential time-saving means for larger-scale operations.

The figure below illustrates the type of graphical depiction of the ID relationships and elements that could be derived from the database and could be used to feed into the Kmap. *This example considers an ISR collection system (UAS) as one element without further decomposing it into its collection platform, its control and processing facilities, etc.*

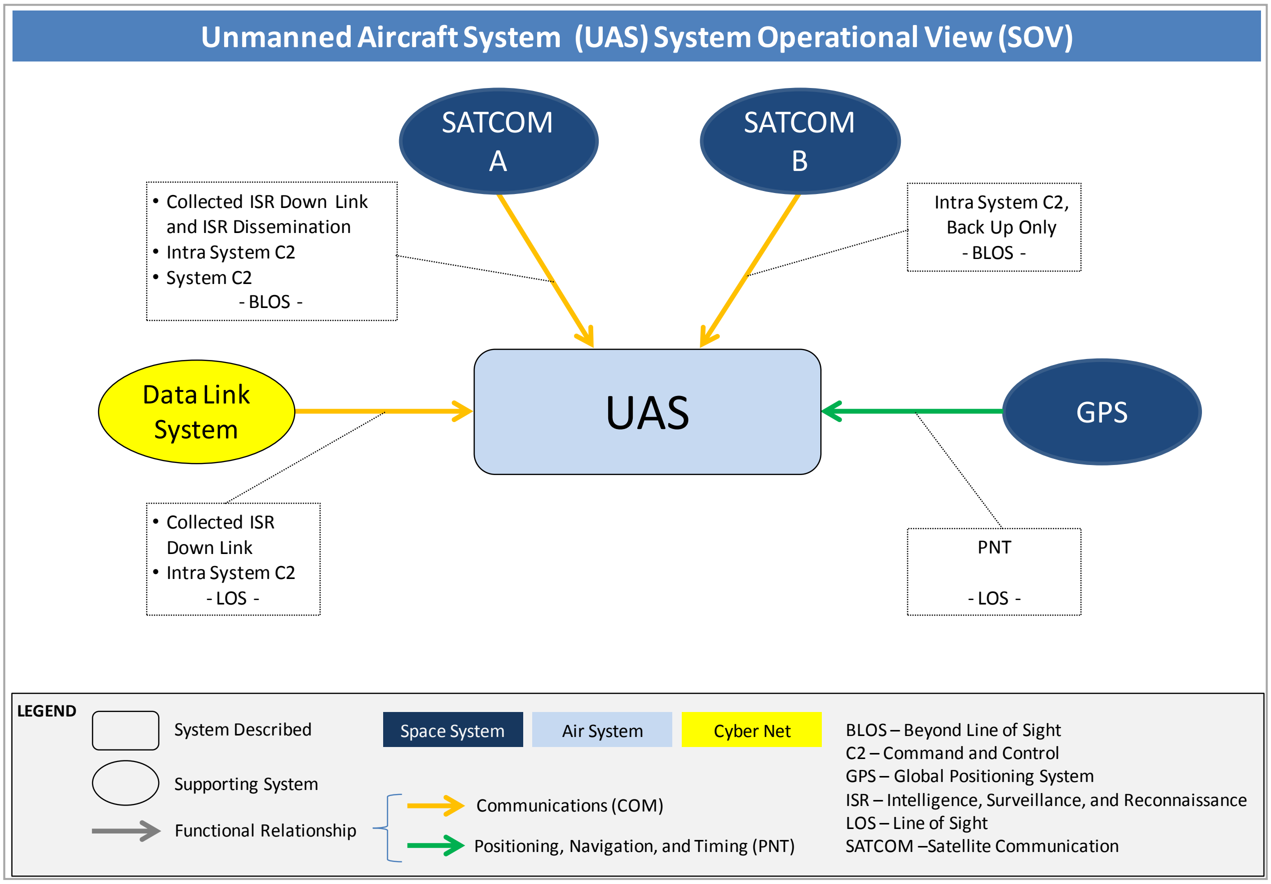

Unmanned Aircraft System (UAS) System Operational View (SOV)
SATCOM A
SATCOM B
• Collected ISR Down Link and ISR Dissemination
• Intra System C2
• System C2
- BLOS -
Intra System C2, Back Up Only
- BLOS -
Data Link System
UAS
GPS
• Collected ISR Down Link
• Intra System C2
- LOS -
PNT
- LOS -
LEGEND
System Described
Supporting System
Functional Relationship
Space System
Air System
Cyber Net
Communications (COM)
Positioning, Navigation, and Timing (PNT)
BLOS – Beyond Line of Sight
C2 – Command and Control
GPS – Global Positioning System
ISR – Intelligence, Surveillance, and Reconnaissance
LOS – Line of Sight
SATCOM –Satellite Communication

Figure 11: System Operational View

b. **Identify and display ID relationships of the supporting systems themselves** by using to the same approach as explained in the previous sub-step (*for example, display ID relationships of the SATCOM A supporting the UAS X*).

c. **Complete the build-up of the Kmap by connecting these various SOVs** in order to constitute a comprehensive web of ID systems and relationships at the function level. These connections should be made on each Kmap, and also among the Kmaps that "share" common supporting systems. This is done by identifying the supporting systems that are common to several system operational views, which in turn enables the identification of nodes that support several systems. *For example, the UAS system requires SATCOM A to transmit its sensor data, and SATCOM A is also required to reach forward nodes of the intelligence mission network.*

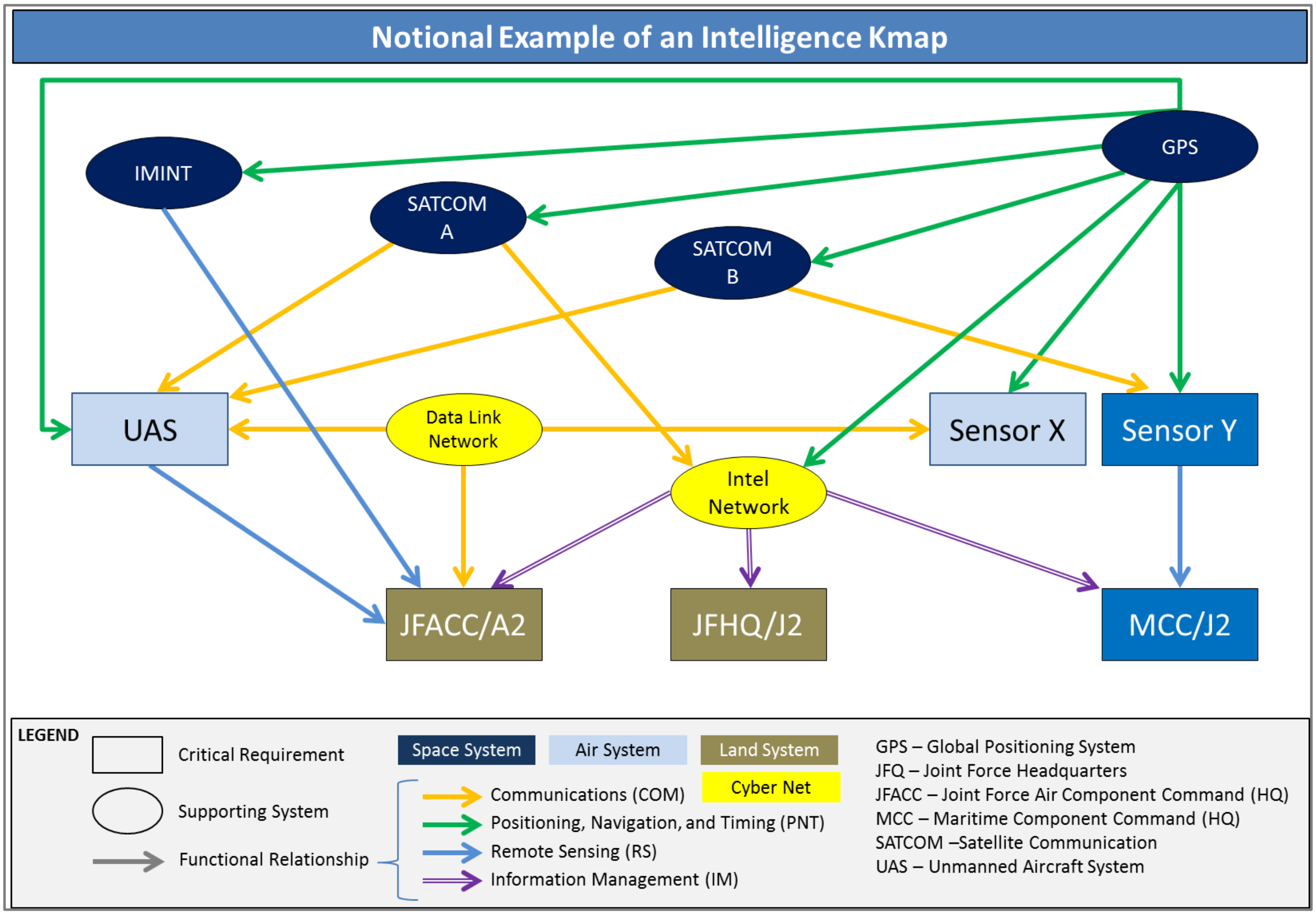

Notional Example of an Intelligence Kmap
IMINT
SATCOM A
SATCOM B
GPS
UAS
Data Link Network
Intel Network
Sensor X
Sensor Y
JFACC/A2
JFHQ/J2
MCC/J2
LEGEND
Critical Requirement
Supporting System
Functional Relationship
Space System
Air System
Land System
Cyber Net
Communications (COM)
Positioning, Navigation, and Timing (PNT)
Remote Sensing (RS)
Information Management (IM)
GPS – Global Positioning System
JFQ – Joint Force Headquarters
JFACC – Joint Force Air Component Command (HQ)
MCC – Maritime Component Command (HQ)
SATCOM –Satellite Communication
UAS – Unmanned Aircraft System

Figure 12: Notional Example of an Intelligence Kmap

d. Depending on the availability of time and expertise, **develop more detailed system operational views**, in order to support the **development of the Kmap**. These detailed SOVs delve into the functional and physical ID relationships among the elements of selected systems and between these elements and supporting systems.

These selected systems should include:

- The CoG critical requirements;
- The most important nodes as identified on the Kmap in the previous sub-step;
- Among these critical requirements and nodes, more particularly the inter-domain "distributed" systems whose elements are located in various domains and rely on their own enabling relationships, according to specific conditions (*the best example is provided by MALE/HALE UAS whose air vehicle and mission control station each have their own communications relationships).*

These detailed SOVs are to be drawn up from information provided in various sources, including staff estimates and capability providers, as well as the ID systems databases if they are developed in advance. They should be annexed to each considered system on the Kmap in order to enable an operator to seek more detailed information for a given system as required.

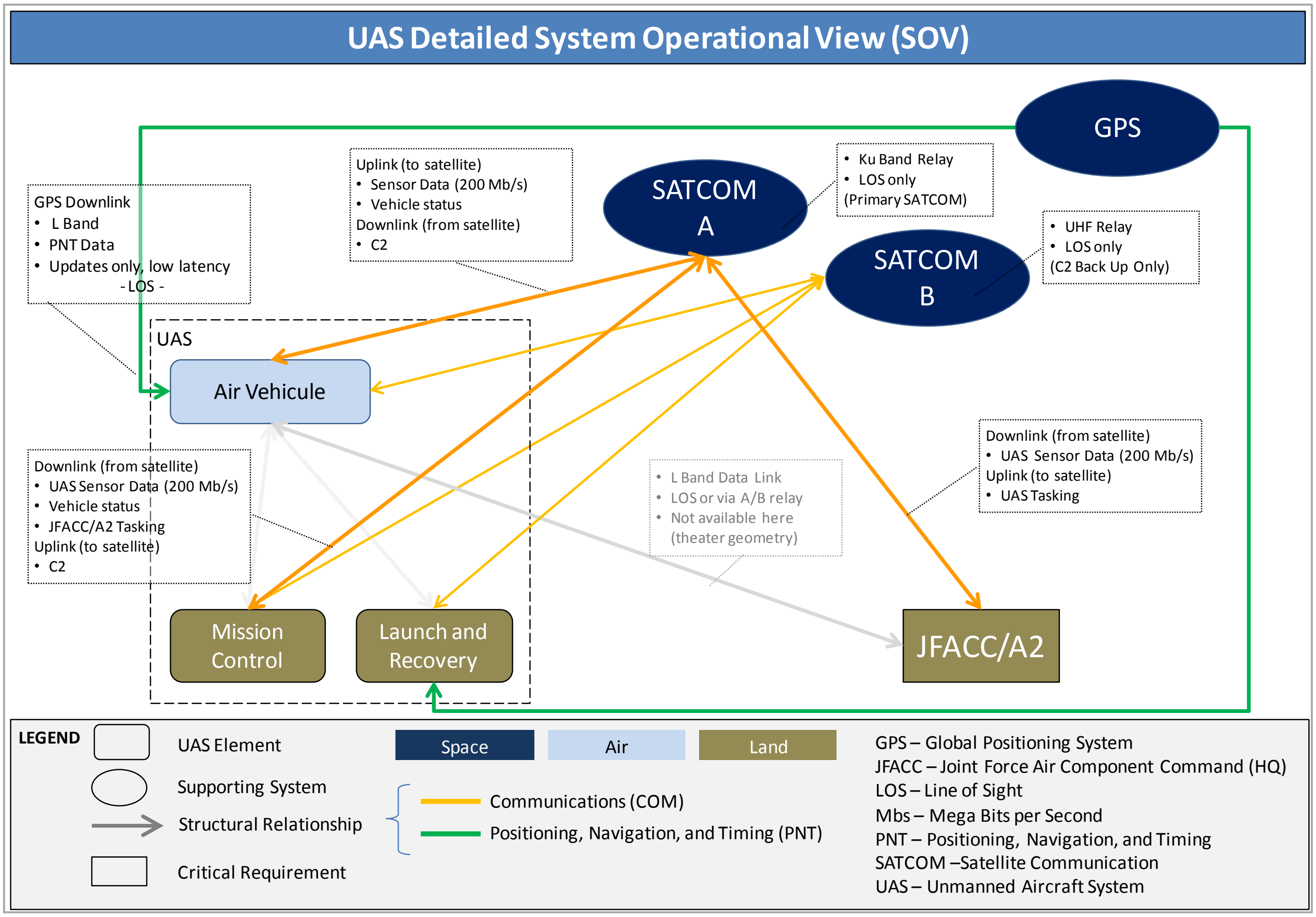


Figure 13 - Example of detailed SOV for a UAS

2.4 Step 4: Analysis of ID Dependencies

The objective of this step is to analyze the relationships among all the considered systems, in order to **determine the enabling ID relationships and dependencies based on the nature of the operational environment**. This can be done by following the sub-steps below.

a. For all relationships of each system depicted in the Kmap[22], **analyze the consequence of a failure of (or the absence of) the functional relationship** on the ability of the considered system to fulfill its tasks, by detailing more specifically:

- The task that could be affected by a potential failure;
- The effect of the potential failure (for example: would it destroy, degrade, disrupt, the ability of the supported system to perform the given task?);
- The timeframe of the effect, which encompasses three criteria:
  1. time-sensitivity/latency (immediate/differed);
  2. frequency (continuous/intermittent);
  3. duration (short/mid/long duration);

[22] The Kmap should already filter out the systems that could be unavailable.

- Whether there are existing alternatives for the given system to offset this failure or whether there are degraded ways to complete the intended task.

This analysis seeks first to determine **whether the relationships are enabling or enhancing**:

- If a given system cannot continue to fulfill its expected task as intended in case of failure of this relationship, the relationship with a given supporting system is characterized as an enabling relationship;
- If the relationship simply improves the performance of the system, the relationship can be qualified as enhancing.

Once the enabling relationships have been determined, **the next step is to identify which ones create dependencies.** The dependency of a system must be analyzed in relation to the capabilities that it requires (communications, PNT, etc.) and the systems that provide them. A system A is qualified as dependent on a system B if it is solely enabled by system B for a given capability and has no alternative ways to mitigate or offset a failure of this single enabling relationship.

The result of this sub-step should be a statement of the enabling relationships and dependencies for each system. This analysis would be captured by both a textbox on the Kmap and a separate textual summary.

Notional example: the HALE UAS system

For example, a HALE UAS is considered to be a critical requirement for the MET "establish situational awareness" as it represents the primary GEOINT collection asset of the A2/JFACC (here the JFACC would be a critical requirement).

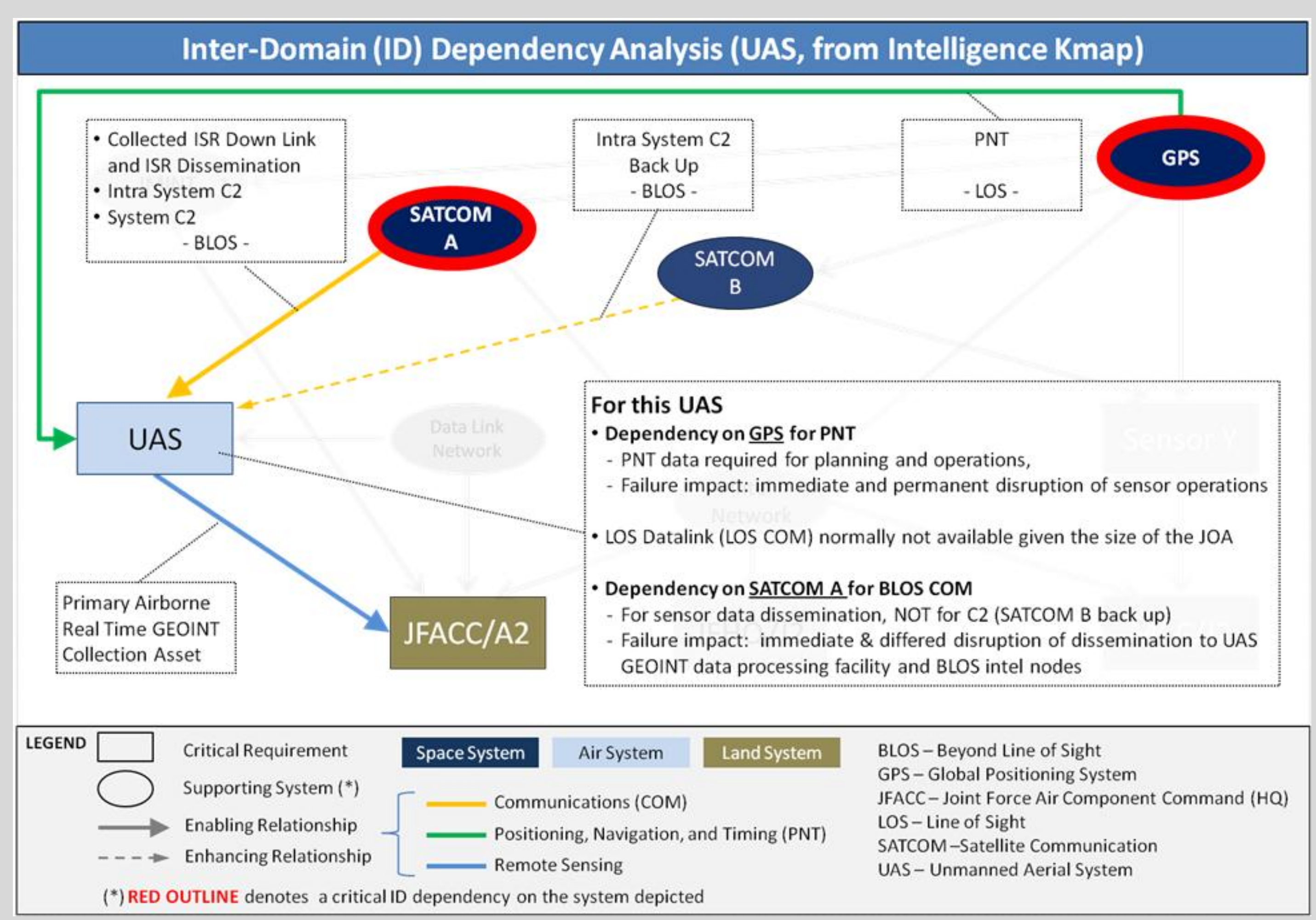
The UAS has several supporting capabilities (see Figure 14):

- ***<u>Communications</u>:***
  - *LOS: One relationship (datalink E); Considered unavailable given the size of the JOA;*
  - *BLOS - SATCOM A: considered available; however, its failure would have the following effect:*
    - *An immediate disruption of UAS support to dynamic targeting applications and a differed degradation for situational awareness and deliberate targeting*
    - *No degradation of UAS C2 as SATCOM B provides a backup solution*

    SATCOM A is categorized as an enabler
  - *BLOS - SATCOM B: considered to be available. Its failure would have no disruptive effect on UAS X operations*

    SATCOM B is categorized as an enhancer;

    <u>For the communications capability: the UAS is dependent on SATCOM A</u>
- ***<u>PNT</u>:***
  - *The UAS relies exclusively on GPS, which is therefore an enabler;*
  - *The UAS has an internal inertial navigation system but it is insufficient to prevent navigation errors in case of a failure of GPS, which would have catastrophic consequences over adversary-controlled areas. For PNT, the UAS is dependent on GPS.*
- ***<u>Conclusion</u>****: in the context of the engagement UAS X is dependent on SATCOM A and GPS.*



Inter-Domain (ID) Dependency Analysis (UAS, from Intelligence Kmap)

- Collected ISR Down Link and ISR Dissemination
- Intra System C2
- System C2

- BLOS -

Intra System C2 Back Up - BLOS -

PNT - LOS -

Primary Airborne Real Time GEOINT Collection Asset

For this UAS

- **Dependency on GPS for PNT**
  - PNT data required for planning and operations,
  - Failure impact: immediate and permanent disruption of sensor operations
- LOS Datalink (LOS COM) normally not available given the size of the JOA
- **Dependency on SATCOM A for BLOS COM**
  - For sensor data dissemination, NOT for C2 (SATCOM B back up)
  - Failure impact: immediate & differed disruption of dissemination to UAS GEOINT data processing facility and BLOS intel nodes

LEGEND

□ Critical Requirement

○ Supporting System (*)

→ Enabling Relationship

- - → Enhancing Relationship

Space System | Air System | Land System

Communications (COM)

Positioning, Navigation, and Timing (PNT)

Remote Sensing

(*) RED OUTLINE denotes a critical ID dependency on the system depicted

BLOS – Beyond Line of Sight
GPS – Global Positioning System
JFACC – Joint Force Air Component Command (HQ)
LOS – Line of Sight
SATCOM –Satellite Communication
UAS – Unmanned Aerial System

Figure 14: Illustrative Example of ID dependencies for the UAS X, as Part of the Intel Kmap

b. **Identify those systems which represent critical ID dependencies**. The critical ID dependencies are essential to the achievement of the mission. A critical ID dependency can be identified:

- In the perspective of each CoG critical requirement, for which an ID dependency is deemed to be critical when:
  - A supporting system has a single enabling relationship with one or several systems constituting critical requirements,
  - A supporting system has a single enabling relationship with one or more other systems enabling the critical requirement,
  - When a large number of systems needed to fulfill a given military function depend on the same enabler, the failure of which would have an adverse cumulative impact on the accomplishment of the mission.
- This analysis of critical ID dependencies should be supported by knowledge maps and could be captured by a table as illustrated below.

MET/CC CoG	Critical Requirements	Critical ID Dependencies	Rationale
Establish situational awareness	Airborne sensors	GPS	Single PNT enabler for all airborne collection systems.
	UAS	SATCOM A	UAS single enabler for communications of collected ISR data

Table 1: Summary of MET/CoG CC–Related Critical ID Dependencies

Although this ID dependencies analysis is mainly conducted during mission analysis, it should be updated as required during COA development, for each COA developed by the joint planning group, particularly based on changes to critical ID-related supporting capabilities for a specific COA. Based on the original operational design and the initial sketch of the considered COAs, this dependencies analysis should seek to highlight the dynamic changes of dependencies between the envisioned phases of the engagement. It may be supported, as required, by differentiated Kmaps for each COA and/or phase of the engagement.

3. Outputs of Module 2

The outputs of this module are:

- The list of critical ID related supporting capabilities;
- Refined list of stakeholders and capability providers;
- The table of the critical ID dependencies to complement the CoG critical requirements;
- The Kmaps depicting the enabling ID relationships and ID dependencies to be used in module 3 for the determination of the critical ID vulnerabilities[23].

* * *

[23] These last outputs go to the intelligence/KD staff.

Intentionally Blank

Module 3: Critical Inter-Domain Vulnerabilities Identification

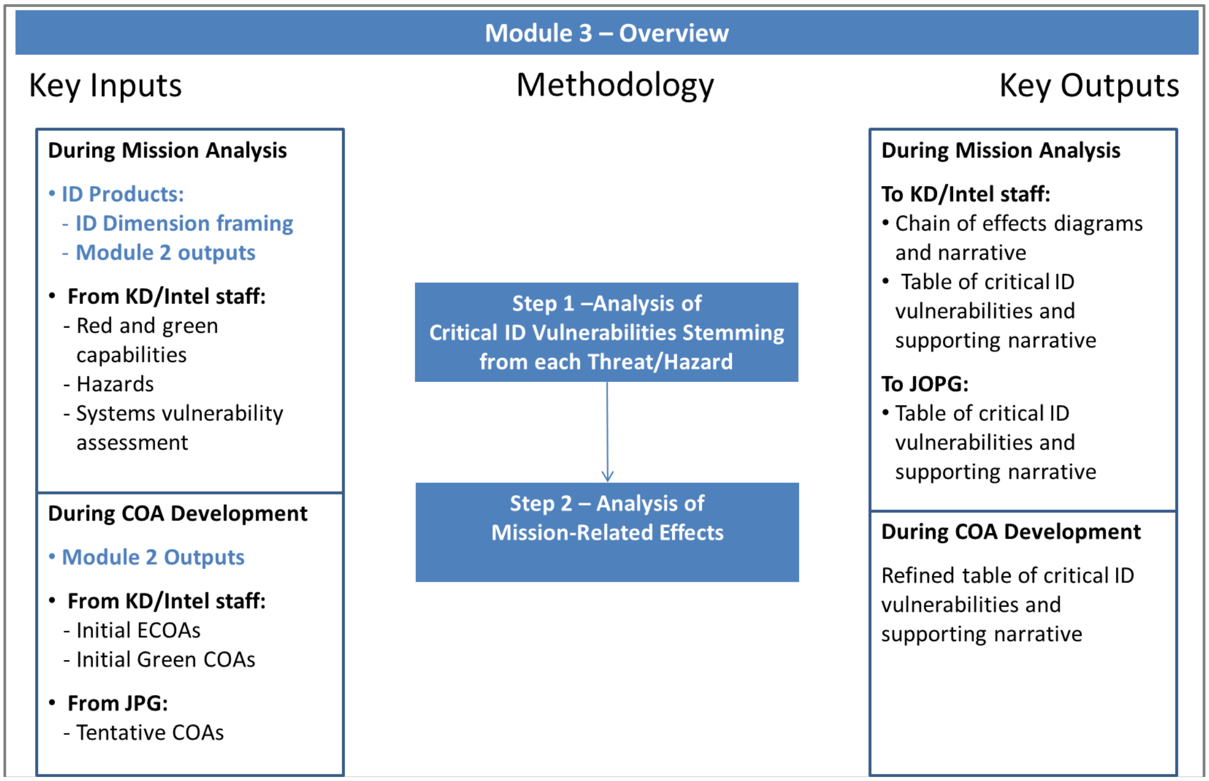
A **critical ID vulnerability** is the vulnerability of a system that constitutes a critical ID dependency due to the fact that it is essential to the achievement of the mission.

The analysis of the critical ID vulnerabilities should first be undertaken during mission analysis relative to the mission essential tasks and the CoG critical requirements. It should then be refined during course of action (COA) development in order to identify the risks associated with the COAs.

It is an iterative effort that is undertaken throughout the planning process. It is intended to feed

- During mission analysis:
  - The analysis of the CoG critical vulnerabilities;
  - The initial risk analysis developed at the end of the mission analysis;
  - The development of the Enemy COAs (ECOAs) and, as applicable, Green COAs;
- During COA development:
  - The development of Blue COAs;
  - As required, the Blue COA analysis;
  - The COA comparison and the operational risk assessment.

The figure below represents the key inputs to module 3, its methodology and its expected outputs.



Module 3 – Overview

Key Inputs

During Mission Analysis

- **ID Products:**
  - **ID Dimension framing**
  - **Module 2 outputs**
- **From KD/Intel staff:**
  - Red and green capabilities
  - Hazards
  - Systems vulnerability assessment

During COA Development

- **Module 2 Outputs**
- **From KD/Intel staff:**
  - Initial ECOAs
  - Initial Green COAs
- **From JPG:**
  - Tentative COAs

Methodology

Step 1 –Analysis of Critical ID Vulnerabilities Stemming from each Threat/Hazard

Step 2 – Analysis of Mission-Related Effects

Key Outputs

During Mission Analysis

To KD/Intel staff:

- Chain of effects diagrams and narrative
- Table of critical ID vulnerabilities and supporting narrative

To JOPG:

- Table of critical ID vulnerabilities and supporting narrative

During COA Development

Refined table of critical ID vulnerabilities and supporting narrative

Figure 15: Module 3 Overview

1. Inputs to Module 3

During mission analysis, the analysis of the critical ID vulnerabilities should start with:

- The outputs of module 2, including the Kmaps and the table of critical ID dependencies;
- The vulnerabilities identified in the POE products. Indeed, the POE identifies the threats and hazards that could affect elements or the systems themselves, including those that represent critical ID dependencies as identified in module 2. It includes specifically:
  - A vulnerability assessment related to the information systems,
  - An analysis of the most plausible hazards, as completed during the description of the impact of the operational environment (POE step 2);
  - The Red and Green capabilities expressed in terms of broad COAs, as completed at the end of the evaluation of the actors (POE step 3).

During COA development, additional inputs include:

- The most probable and most dangerous ECOAs as developed in POE step 4;
- The initial sketch of each COA (or tentative COAs), developed by the joint planning group;
- The refined outputs of module 2 based on these COAs.

2. Module 3 Method

Based on the vulnerabilities identified in the POE products, this module determines the critical ID vulnerabilities. The method is divided in two steps:

- The first step analyzes the chain of effects stemming from each system that is vulnerable to threats or hazards;
- The second step correlates these chains of effects for each mission essential task and CoG critical capability (during mission analysis) or for each COA (during course of action development).

2.1 Step 1: Analysis of Effects Stemming from Each Threat or Hazard

The aim of this step is to determine the expected effects and ultimately the criticality of a potential attack or a hazard on a vulnerable system on the ability of the force to execute the METs and on the CoG CC capabilities that rely on this vulnerable system through the ID relationships.

Based on the enabling ID relationships identified in module 2, this step involves analyzing the chains of effects that would stem from each potential threat or hazard. The priority of the analysis should be on the vulnerable systems that represent a critical ID dependency. However, other vulnerable systems should also be considered because it is possible that an attack or a hazard may achieve an effect by indirectly affecting the critical ID dependency through another supporting system. *For example, a given CWAN representing a critical dependency for the C2 function may be indirectly affected by offensive actions against a SATCOM which enables this CWAN.*

Once the analysis of the chain of effects is completed, a judgment is made regarding the criticality of the vulnerability, based on the severity of the potential effect on the ability to execute a MET and on the CoG critical capabilities (during mission analysis) or the COA (during COA development).

This step should result in an initial **list of critical ID vulnerabilities**. This list could already be used by planners to begin thinking about mitigation options.

This analysis qualifies direct and indirect effects according to two sets of criteria:

- The nature of the effects. The scope and the nature of the effects for a given system depend on the nature and the criticality of the enabling relationships and the existence of other enhancing relationships, as analyzed in module 2. A list of effects that may be used for this analysis is provided in the table below:

Effect	Definition
Degrade	A function's operation is permanently impaired, but the damage does not extend to all facets of the function's operation
Deny	A function's operation is impaired over the short term, but the damage extends to all facets of the function's operation
Destroy	A function's operation is permanently impaired, and the damage extends to all facets of the function's operation
Diminish	To reduce the effectiveness of an activity. This is similar to degrade without the kinetic overtones
Disrupt	A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation
Exploit	To gather information that will enable opposition ability to conduct operations to induce other Effects
Limit	Reduce the options or COAs available to the enemy commander
Neutralize	To render ineffective, invalid or unable to perform a particular task or function
Suppress	Temporary or transient degradation by an opposing force of the performance of a weapons system below the level needed to fulfill its mission objectives

Table 2: Definitions of Effects[24]

- The timeframes associated with these expected effects. This timeframe encompasses three criteria:
  - Time-sensitivity/latency (is the effect immediate or differed?)
  - Frequency (how often does it occur? Is it continuous or intermittent?)
  - Duration (how long would the effect last? Short, mid to long duration?)

An approach to analyze the critical ID vulnerabilities could be to apply the following sub-steps:

[24] Source: "Targeting Effects Definitions" in USJFCOM, Joint Warfighting Center, Joint Fires and Targeting Handbook, 19 October 2007, pp. III-38-39

a. **Assess the direct effects of each threat and hazard**:
   - Review the threat and hazards provided by the POE;
   - Select, among the vulnerable systems, those that constitute critical ID dependencies;
   - Qualify the direct effect of the considered threat and hazard:
     - On the vulnerable system taken as a whole;
     - On the capability it provides.

   For example: the POE states that "the adversary has the capability to jam the GPS signal over area X". The effect, as identified in this sub-step would be: the GPS is denied over area X but not over the rest of the JOA; PNT is degraded over area X for air assets and not affected over the rest of the JOA.

b. Assess the indirect effects of each threat and hazard:
   - Select, on the relevant Kmaps, the enabling ID relationships stemming from the systems that are assessed to be vulnerable in the POE;
   - In order to develop the chains of effects, qualify the indirect effects on:
     - Dependent systems;
     - Critical ID-related supporting capabilities;
     - Ultimately, the METs or CoG critical capabilities (or on the COAs is this analysis is done during COA development).

This analysis of the chains of effects should be:

- Supported by the Kmap to guide the identification of elements and relationships to be considered for the chains of effects;
- Developed through causal diagrams of effects.

c. **Identify a first set of critical ID vulnerabilities**:
   - Distinguish the chains of effects which are the **most time-sensitive** or could lead to the **most dangerous effects** for the considered MET and CoG critical capabilities or for the considered COA;
   - Qualify the vulnerable systems at the source of these chains of effects as critical ID vulnerabilities.

Capture results in a narrative (explaining the critical ID vulnerabilities, their characteristics and potential effect) and a supporting table.

Example*: In module 2, analysts identified GPS as a critical dependency for the chains of dependencies related to two mission essential tasks: "conduct area interdiction" (AI) and "establish situational awareness" (SA). The POE evaluated that a Red actor has the capability, the probable intent and the will to locally jam the GPS signal. The analysts therefore develop the chain of effects corresponding to these threats following the chains of dependencies mentioned above. In this example, the most adverse effect of the local jamming of the GPS signal would concern the cruise missiles' navigation and precision guidance for the AI MET and airborne ISR sensors for the SA MET, other assets having less reliance on GPS. The conclusion is that the GPS signal represents a critical ID vulnerability for MET AI as it neutralizes the potential use of a key asset, but does not represent a critical vulnerability for MET SA, which is also supported by naval and space sensors.*

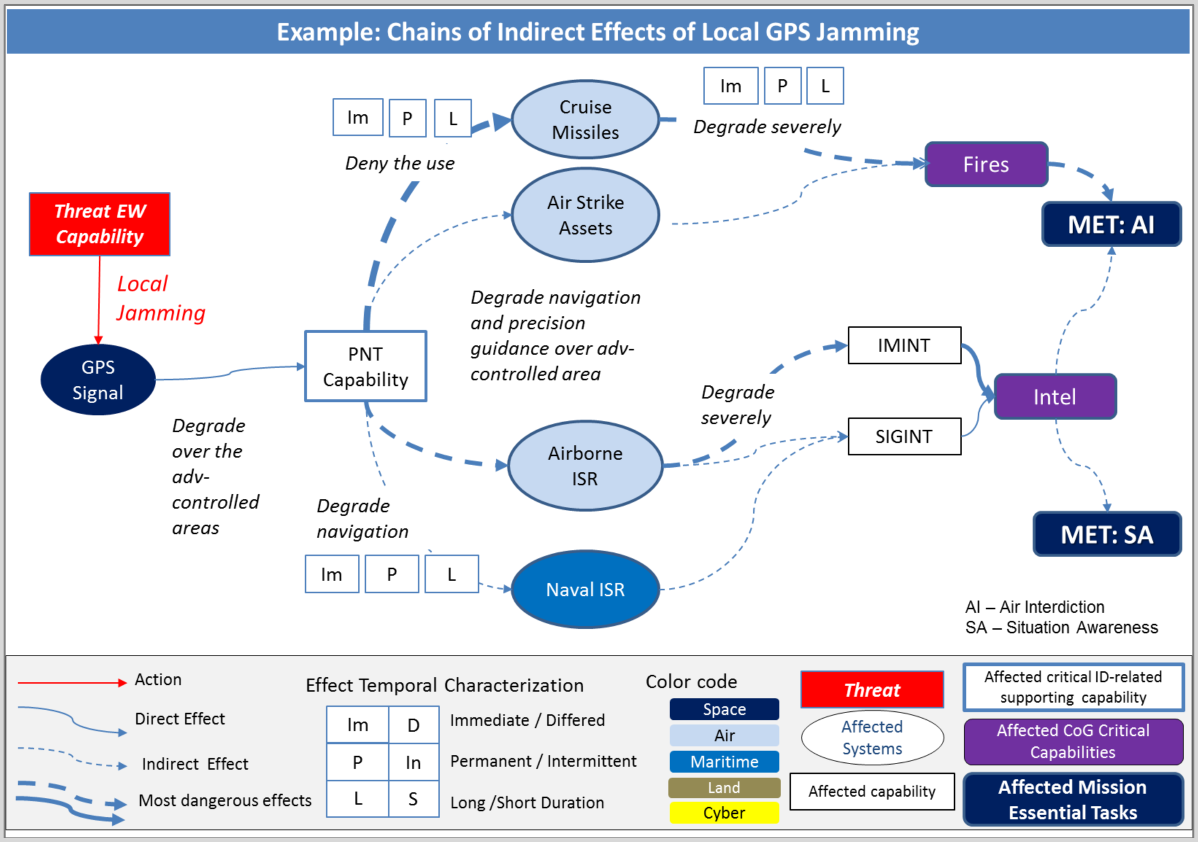


Figure 16: Illustrative Diagram of a Chain of Indirect Effects Caused by Local GPS Jamming

In this example the table summarizing this analysis would contain the following elements:

Threat/Hazard & Critical Vulnerability	Main Effects	Criticality for MET/CoG CR
Red capability: local jamming **CV: GPS signal**	• Neutralize use of cruise missile • Neutralize airborne IMINT sensors	MET AI: Critically degraded Too few other air strike assets to overcome Red defense
		MET SA: Partially but non critically degraded Availability of space and naval sensors

Table 3: Summary of Critical Vulnerabilities per Threat/Hazard

2.2 Step 2: Analysis of Mission-Related Effects

This step aims to refine the identification of critical ID vulnerabilities for each MET and CoG critical capability during mission analysis or for each COA during the COA development. Indeed, for a given MET or CoG CC or for a given COA, there may be several probable vulnerabilities. Indirect effects on one system, stemming each from separate vulnerabilities to direct effects, may reinforce one another. *For example, the combination of a computer network attack on the vulnerable piece of a CWAN and the spoofing of the GPS signal, together, may reinforce the negative effects on a coalition C2 node.*

This analysis is carried out by correlating the chains of effects developed in step 1 of this module (for each given MET or CoG critical capability during mission analysis or for each COA during COA development), then by refining the critical ID vulnerabilities. This may be undertaken by applying the following sub-steps:

a. **Correlate effects**:
   - Select, from the results of step 1, all the chains of effects pertaining to a considered MET/CoG CC or COA;
   - Identify those systems which are affected by several effects;
   - Analyze how these effects reinforce or mitigate one another for the considered system;
   - Refine the qualification of the indirect effects according to the same criteria used in step 1,
     - Determine whether a system that constitutes a critical ID dependency is more severely affected by this combination of effects;
     - Draw conclusions regarding the time-sensitiveness and most dangerous effects for the MET and CoG CC or COA.

b. **Refine the critical ID vulnerabilities**: based on the correlation of effects, review and confirm whether the vulnerable element at the source of the chain of effects should still be considered a critical ID vulnerability.

c. **Propose risk mitigation options**: based on the outputs of modules 2 and 3, and drawing on the Kmaps, the staff may propose risk mitigation options to the joint planning group to reduce these critical ID vulnerabilities. These mitigation options may address the reliance on other enabling or enhancing relationships or the conditions of the use of the supporting systems.

To perform this analysis, the staff may fuse the different causal diagrams of chains of effects into a classical KD influence diagram or conduct an open discussion to compare these chains of effects or a combination of both. The critical factor will be the time available to analysts and the number of chains of effects to be correlated.

The analysis is captured by a written summary and a table.

Example: the "conduct area interdiction over the JOA" MET may be affected by two chains of effects: the "GPS local jamming" (see step 1 example) and a hazard, the solar wind which is expected to disturb satellite signal.

1. *The GPS signal is jammed locally but also degraded intermittently by solar wind;*
2. *Combined indirect effects on air strike assets and cruise missiles dependent on PNT leads to the suppression of the interdiction critical capability;*
3. *The solar wind also intermittently degrades the links of a SATCOM system;*
4. *The effect on SATCOM leads to a degradation of the long-haul connection required for effective CWAN supporting coalition C2;*
5. *Airborne and naval ISR sensors are affected by both chains of effects leading to degraded ability to produce IMINT and to lesser extent on SIGINT.*

The correlation of the chains of effects leads to the identification of airborne collection assets as complementary critical ID vulnerabilities and to the conclusion that the ability to perform the MET AI is significantly degraded.

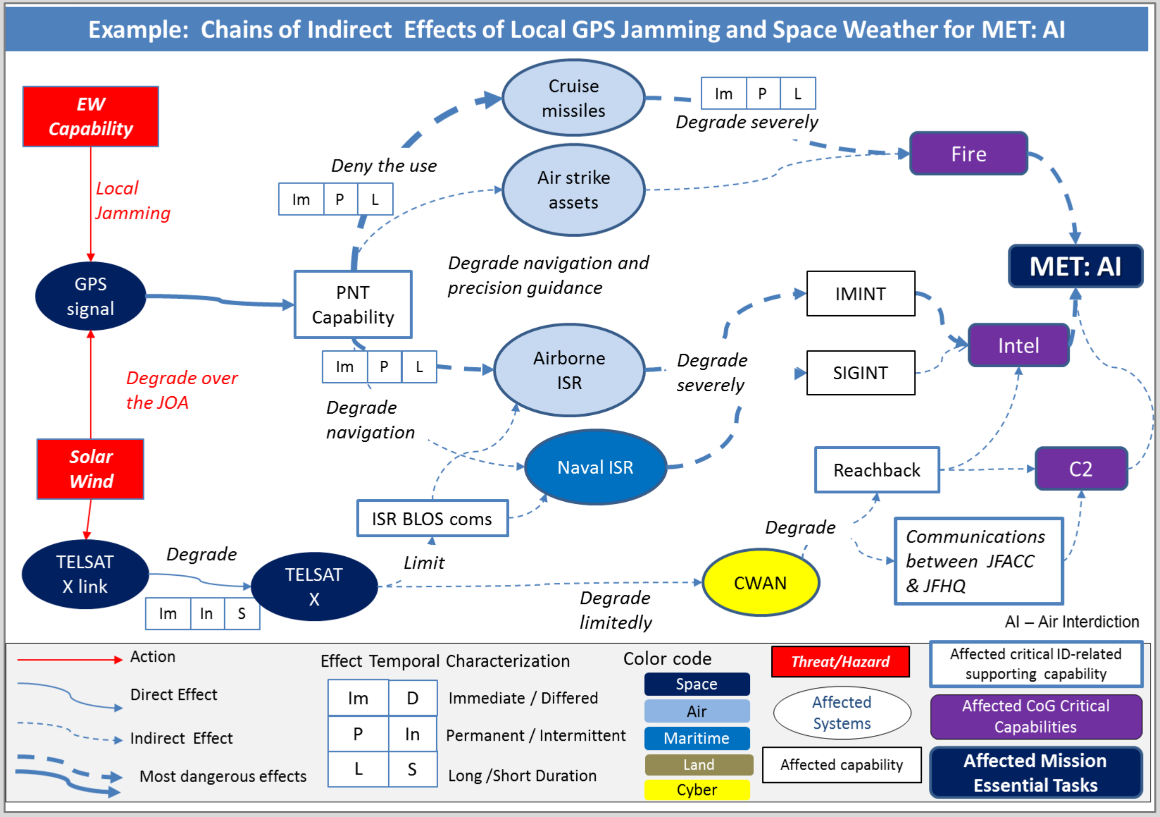


Figure 17: Influence Diagram of Correlated Chains of Indirect Effects

In this example, the table summarizing this analysis could state:

MET / CoG CC	Overall Effect	Criticality ID Vulnerabilities	Risk Mitigation Options
Conduct Area Interdiction	Significantly degraded	source of the chains of effects: • GPS Signal • Space systems affected by solar winds	• Rely primarily on naval SIGINT collection assets • Rely on air strikes assets with non-GPS guided munitions
		Other assets: • Cruise missiles • Airborne ISR sensors	

Table 4: Summary of MET/CC CoG – Related Critical ID Vulnerabilities

3. Outputs of Module 3

The outputs of this module are:

1) **During mission analysis**
    a. **To the joint planning group:** the table of the critical ID vulnerabilities feeds the analysis of the CoG critical vulnerabilities, the initial risk analysis that is performed at the end of the mission analysis and the development of risk mitigation options;
    b. **To the KD/Intel staff:** the chain of effects diagrams and written narrative statements as well as the table of the critical ID vulnerabilities. These diagrams support the development of the ECOAs and the identification of the most dangerous one.

2) **During COA development**
    a. To the **joint planning group**:
        i. a refined table of critical ID vulnerabilities for each tentative/initial sketch of Blue COAs, Blue and as required and Green COAs;
        ii. As required, another refined table of critical ID vulnerabilities stemming from the COA gaming as action/reaction/counter-reaction analysis may highlight new unexpected critical ID vulnerabilities;
        iii. Ultimately, critical ID vulnerabilities should be considered among the criteria retained for the COAs comparison;
    b. To the **KD/Intel Staff**: the chains of effects diagrams.

* * *

Appendix A – Illustrative Example

Please note: the sole purpose of this fictional example is to facilitate understanding of the methodology developed in MNE 7 Outcome 4 by providing a concrete illustration. While it mentions real systems in order to make the illustration more tangible, it is NOT intended to portray any real enabling relationships or dependencies between these systems.

In the description of each module, *text in italic font designates work that would normally be undertaken by a commander and his/her staff in normal analysis and planning processes*. Plain font is used to designate results of the application of the methodology, and the way that these results would enrich traditional planning processes.

1. Context

A Red regional power represents a threat for neighboring Green states. They are separated by a strait, through which an important part of the regional oil production transits. The Red power unilaterally claims control of the strait and begins aggressive patrol activities. Many countries decide to boycott Red's oil exports and the UN Security Council (UNSC) imposes sanctions in the hopes of compelling Red to change its behavior. However, due to a complex internal situation, Red retaliates by blockading the strait, thereby jeopardizing the regional economy and generating a new oil crisis. Emerging powers who initially supported Red at the beginning of this protracted diplomatic and economic crisis no longer oppose a UNSC resolution initiated by three permanent members of the Council. This resolution authorizes the use of force to re-establish freedom of navigation (FoN) across the strait. A coalition of states, led by the United States, acting upon this UNSC resolution, decides to militarily compel Red to negotiate. The UN resolution explicitly precludes any engagement of ground troops on Red territory and constrains the campaign to air and maritime operations in a manner proportionate with the aim of the resolution.

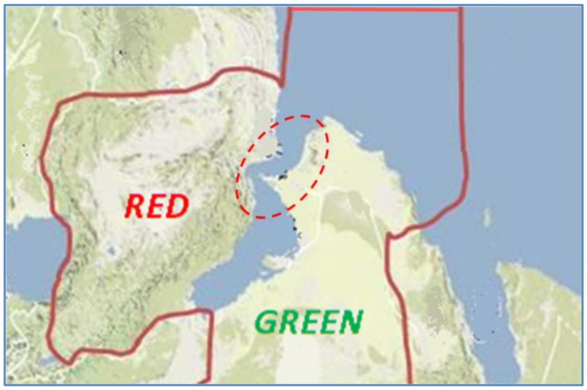
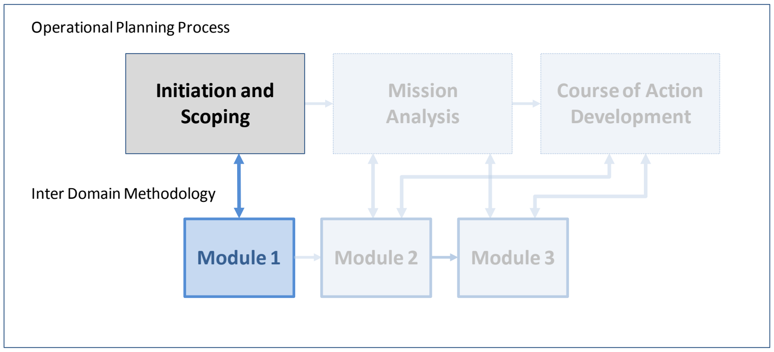


Figure 18 – The Crisis Area

2. Framing the Inter-Domain (ID) Dimension of the Engagement (Module 1)



During the problem framing, nested in the initiation and scoping stage of the operational planning process, the commander and his staff hypothesize that Red will attempt to prevent coalition forces from progressively deploying into and operating in their Joint Operations Area (JOA). One pillar of this strategy is the strategic preclusion of the coalition: Red will deter Green actors from providing basing for coalition forces by leveraging terrorism threats. The second pillar is an operational anti-access and area denial (A2/AD) strategy, which would aim to:

- *Degrade coalition stand-off ISR capabilities;*
- *Hinder coalition offensive air operations;*
- *Prevent the deployment of coalition naval assets to reestablish and maintain freedom of navigation (FoN) in the strait.*

The initial preparation of the operational environment (POE) briefing outlines that Red has some significant computer network operations (CNO) capabilities, as well as limited counter-space ones.

The commander orients his staff on the following domain interactions: how could these CNO and limited counter-space capabilities affect the coalition's ability to prepare and execute FoN air and naval operations? How may these same capabilities disrupt maritime activities in the area if FoN is reestablished?

The exploration of these interactions leads to the formulation of the following ID challenges:

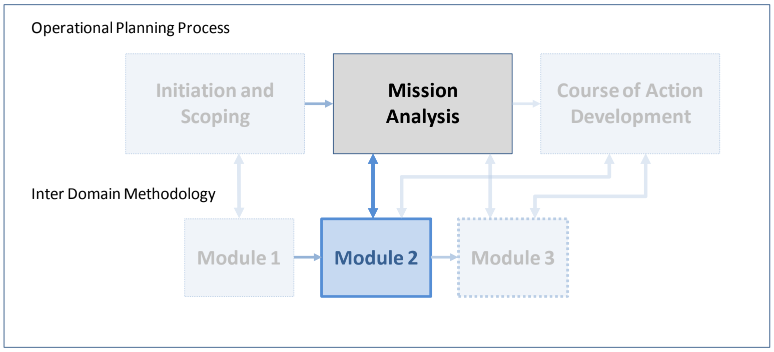
- Possible disruption of space support to C2, Intelligence and Fires capabilities required to conduct FoN operations, and;
- Possible disruption of situational awareness and management of the commercial traffic.

Moreover, the initial appraisal of the operating conditions highlights the fact that there are limited basing options. This entails the need for long range air and naval operations, which should also be very responsive given the threat. These conditions tend to reinforce the criticality of Beyond Line of Sight (BLOS) communications provided by SATCOM and, conversely, lessen the importance of space ISR, at least for real-time Geospatial Intelligence (GEOINT).

The identification of these initial ID considerations within the problem framing point to the need to better understand ID dependencies related to the C2, Intelligence, and Fires military functions as well as to the non-military maritime domain functions in the commander's area of interest.

Each force contributing nation gathers the relevant information about its own capability providers in order to support the subsequent analysis of dependencies. The staff furthermore considers that categories of stakeholders would include Internet providers to Green states, which may be affected or exploited by Red CNO.

3. ID Relationships Mapping and ID Dependencies Analysis (Module 2) – as a Contribution to Mission Analysis



2.1 Module 2 Step 1- Analysis of the Critical ID-Related Supporting Capabilities

During the initial design and concurrent mission analysis, the commander and his staff determine the Mission Essential Tasks (MET) which include (but are not limited to):

- *Establish and maintain situational awareness (SA) of Red naval and air capabilities able to intervene in the strait, as well as of maritime traffic in the strait;*
- *Conduct offensive air operations in the strait's approaches;*
- *Secure and protect sea lines of communication in the Area of operations.*

Furthermore, the commander and his staff determine that the Red operational center of gravity (CoG) is its A2/maritime AD assets. It is assumed that once they are suppressed, Red should be compelled within a short timeframe.

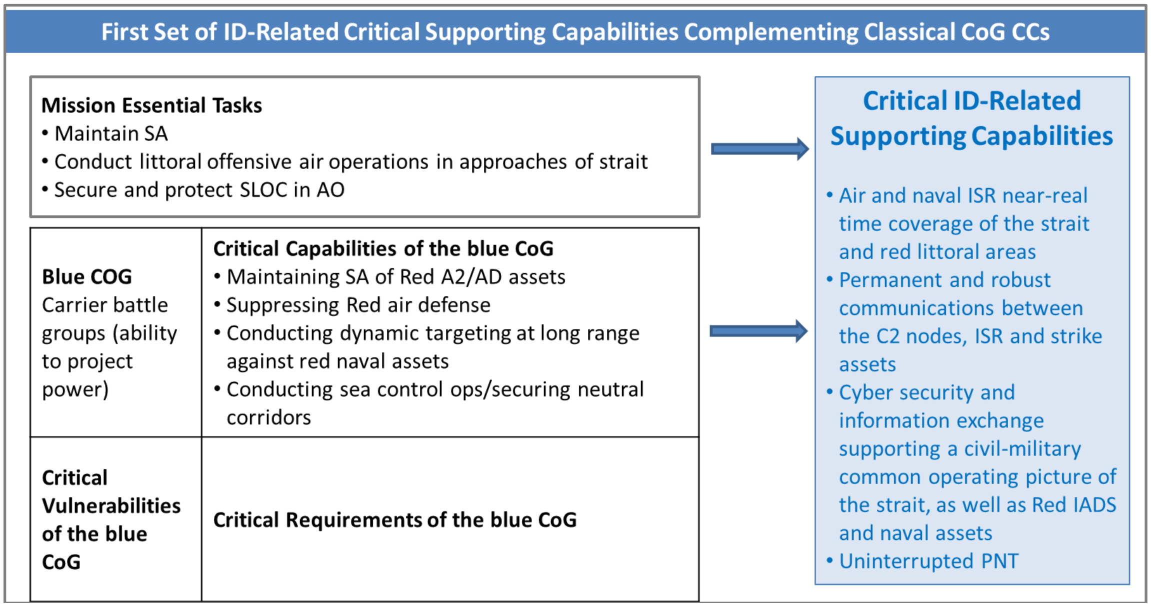
The Blue operational center of gravity is the Carrier Battle Groups (CBG), which are indispensable for the execution of the METs in this context.

The staff determines the CoG critical capabilities (CoG CCs), which include:

- *The ability to maintain situational awareness of Red air and naval capabilities, and of the traffic in the strait when it resumes;*
- *The ability to suppress enemy air defenses, fixed and mobile, along the strait to provide the required freedom of maneuver to coalition air assets;*
- *The ability to execute dynamic targeting at long range against Red naval assets including land-based anti-ship missile capabilities,*
- *The ability to execute sea control operations and secure corridors to cross the strait.*

From these CoG CCs, the staff determines a first set of critical ID-related supporting capabilities, which include:

- Air and naval remote sensing supporting near-real time ISR coverage of the strait and Red threat;
- Permanent and robust tactical communications between sensors, C2 nodes and shooters supporting the dynamic targeting;
- Reliable information exchange means with civilian maritime control centers, and cyber security supporting a civil-military common operating picture of the strait and its approaches;
- Uninterrupted PNT.



First Set of ID-Related Critical Supporting Capabilities Complementing Classical CoG CCs

Mission Essential Tasks
- Maintain SA
- Conduct littoral offensive air operations in approaches of strait
- Secure and protect SLOC in AO

Blue COG
Carrier battle groups (ability to project power)

Critical Capabilities of the blue CoG
- Maintaining SA of Red A2/AD assets
- Suppressing Red air defense
- Conducting dynamic targeting at long range against red naval assets
- Conducting sea control ops/securing neutral corridors

Critical Vulnerabilities of the blue CoG

Critical Requirements of the blue CoG

Critical ID-Related Supporting Capabilities
- Air and naval ISR near-real time coverage of the strait and red littoral areas
- Permanent and robust communications between the C2 nodes, ISR and strike assets
- Cyber security and information exchange supporting a civil-military common operating picture of the strait, as well as Red IADS and naval assets
- Uninterrupted PNT

Figure 19 – First Set of ID-Related Critical Supporting Capabilities Complementing CoG CCs

Based on the CoG critical capabilities and the critical ID-related supporting capabilities, the staff determines a first set of CoG critical requirements (CoG CR), among which:

- *Aircraft carrier, surface combatants and long-range strike assets (air and sea-launched Cruise missiles, SEAD aircraft);*
- *Integrated operational/tactical C2 and intelligence operations structure and assets;*
- *Real time air and naval ISR sensors;*
- *Civilian situational awareness systems.*

These critical ID-related supporting capabilities are further refined or expanded based on the analysis of the operating conditions stemming from POE products as well as the CoG critical requirements.

The size of the JOA, as well as the need to execute long range operations, confirm the emphasis on BLOS rather than LOS communications.

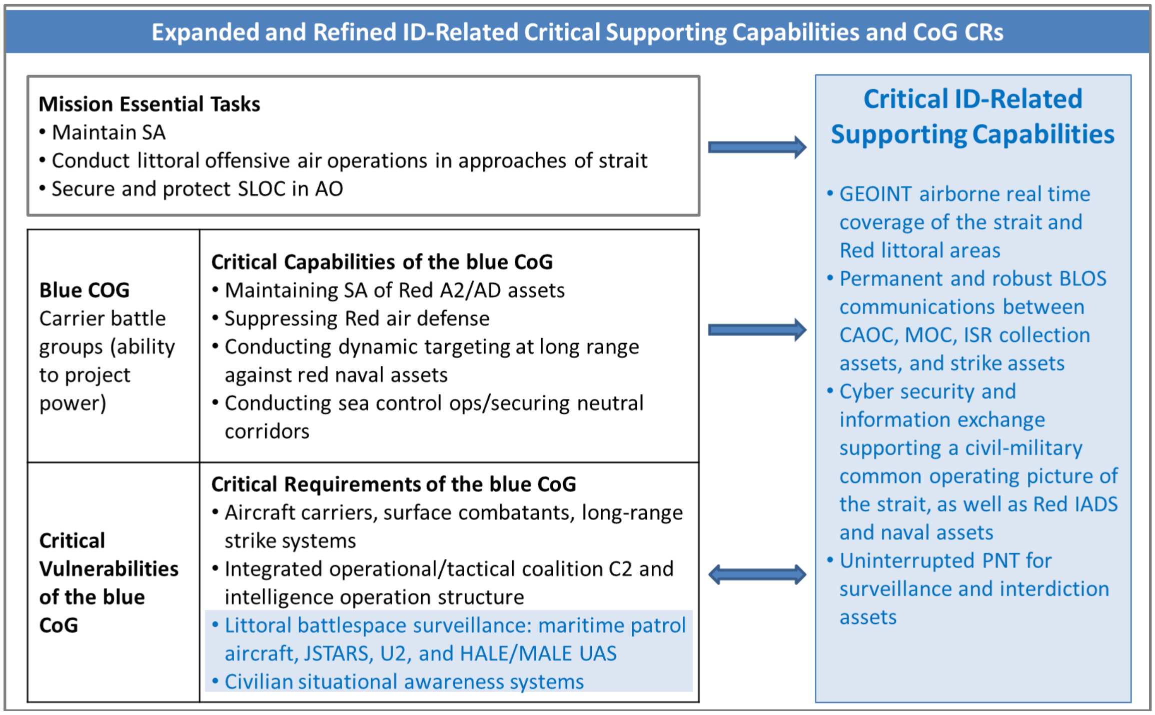
The theater topography shows terrain features that prevent a comprehensive observation of the strait by coalition naval assets. Moreover, Red naval assets are mostly composed of small ships which use swarming tactics but do not require extensive use of communications. This situation emphasizes the use of GEOINT airborne collection capabilities to cover the strait while SIGINT remains the primary ISR discipline to support SEAD operations. The critical ID-related supporting capabilities are thus once again refined and GEOINT airborne near-real time coverage of the strait and red littoral areas is added.

The list of critical ID-related supporting capabilities is therefore established as follows:

- Airborne GEOINT supporting near real-time ISR coverage of the strait and Red threat;
- Uninterrupted communications and Positioning, Navigation and Timing (PNT) capabilities to operate ISR collection, SEAD and interdiction assets;
- Permanent and robust Beyond Line of Sight (BLOS) communications between the Combined Air and Space Operations Center (CAOC), Maritime Operations Center, ISR systems, sea and air-launched cruise missiles and strike assets;
- Information exchange and cyber security to fuse and secure a common operating picture of the strait, to include commercial shipping in the area, and Red naval assets, IADS and anti-ship missiles.

Related CoG Critical Requirements are also refined accordingly. For example:

- Generic ISR sensors are identified more specifically to be littoral battlespace surveillance GEOINT providers including maritime patrol aircrafts, JSTARS, U2 and High Altitude /Low Endurance (HALE) Unmanned Air Systems (UAS) RQ-4 Global Hawk and other Medium Altitude /Low Endurance (MALE) UAS;
- Regional maritime centers and communications, which are key assets to contribute the fusion of a common operating of the strait including commercial traffic.



Expanded and Refined ID-Related Critical Supporting Capabilities and CoG CRs

Mission Essential Tasks
- Maintain SA
- Conduct littoral offensive air operations in approaches of strait
- Secure and protect SLOC in AO

Blue COG
Carrier battle groups (ability to project power)

Critical Capabilities of the blue CoG
- Maintaining SA of Red A2/AD assets
- Suppressing Red air defense
- Conducting dynamic targeting at long range against red naval assets
- Conducting sea control ops/securing neutral corridors

Critical Vulnerabilities of the blue CoG

Critical Requirements of the blue CoG
- Aircraft carriers, surface combatants, long-range strike systems
- Integrated operational/tactical coalition C2 and intelligence operation structure
- Littoral battlespace surveillance: maritime patrol aircraft, JSTARS, U2, and HALE/MALE UAS
- Civilian situational awareness systems

Critical ID-Related Supporting Capabilities
- GEOINT airborne real time coverage of the strait and Red littoral areas
- Permanent and robust BLOS communications between CAOC, MOC, ISR collection assets, and strike assets
- Cyber security and information exchange supporting a civil-military common operating picture of the strait, as well as Red IADS and naval assets
- Uninterrupted PNT for surveillance and interdiction assets

Figure 20 – Expanded and Refined ID-Related Critical Supporting Capabilities and Corresponding CoG CRs

2.2 Module 2 Step 2- Identification of the ID System Elements

For each military function prioritized during module 1 (C2, Intelligence, and Fires), the staff uses the functional models to identify the various systems (the ID System elements) that contribute to the primary and supporting capabilities of the considered function.

Regarding the intelligence function, the systems providing the primary capabilities include:

- The coalition intelligence structure: J2/CJFHQ, A2/JFACC, N2/MOC and reach-back centers;
- The collection assets:
    - The battlespace surveillance systems constituting critical requirements; Global Hawk and MALE/UAS systems (MQ-9 Reapers and Harfang), JSTARS, U2 and P3 maritime patrol aircrafts
    - ASTOR and tactical recce systems such as Rafale Reco-NG and F/A-18 SHARPS
    - Naval SIGINT assets such as SNAs and some surface combatants
    - The space assets: Helios and other national technical means;
- The coalition intelligence information system

The systems providing the ID-related supporting capabilities include

- For PNT: the GPS and eLORAN
- For communications: Global Broadcast Service-related civilian and MILSATCOMs for US BLOS communications, Syracuse and EUTELSAT for French BLOS communications, Link-16 and Link-22 networks, etc.
- For information management: the coalition wide area network.

2.3 Module 2 Step 3 –Mapping of ID Relationships

Drawing from the relevant parts of the systems databases that could have been developed during peacetime, and would then be shared among the force contributing nations, the staff generates the system operational views, with the ID relationships and corresponding supporting systems, of key systems identified in the previous step, which include the RQ-4, MQ-9 and Harfang UAS, air and sea-launched cruise missiles systems and other systems related to the identified critical requirements. They review the availability of the supporting systems. For example, one of the civilian SATCOM systems, which would be required for UAS C2 and data link, does not have the required leasing agreement in place, limiting the ability to operate these ISR collection assets.

For each military function, the staff builds a Kmap which correlates these operational views. In doing so, the staff can identify the supporting systems that are common to several key systems. For example, in the Intelligence Kmap, they identify the EUTELSAT satellite communications system, as it supports both US and French UAS. The staff also identifies cross-functional nodes, such as the GPS for C2, ISR and Fires.

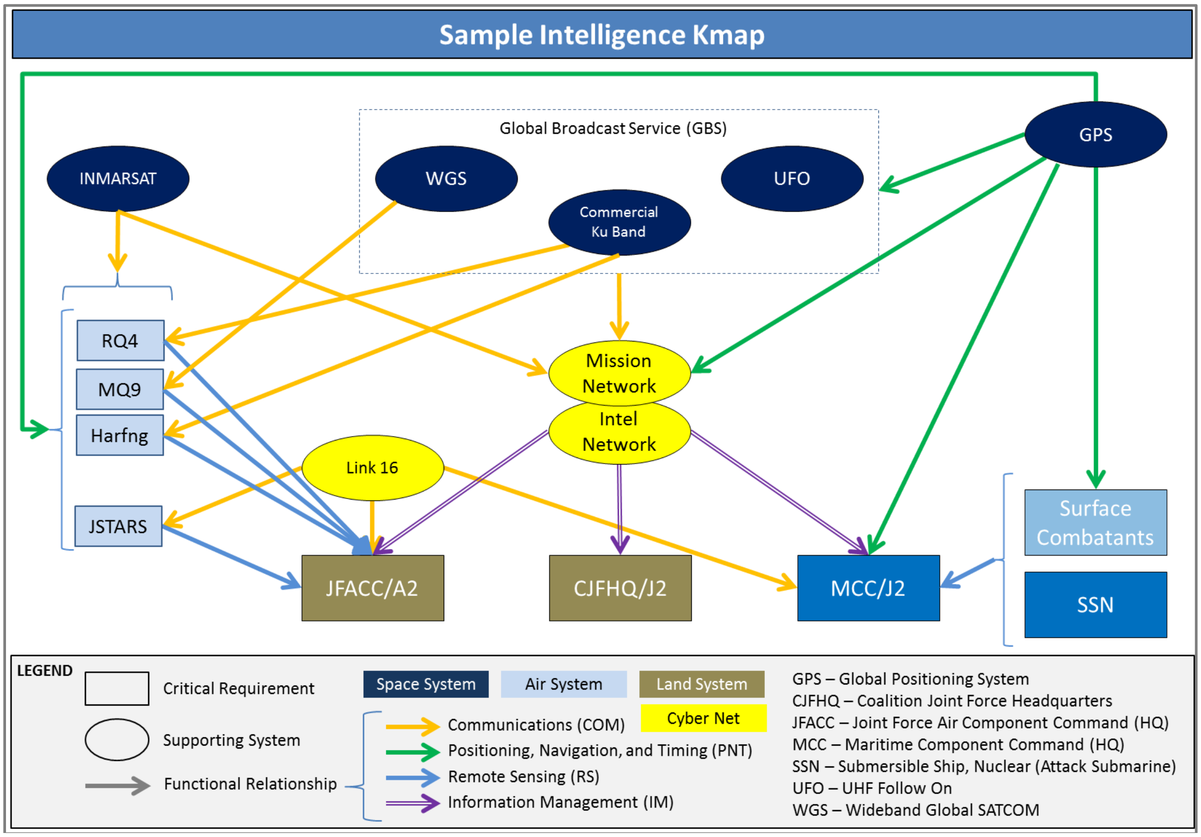

Sample Intelligence Kmap
Global Broadcast Service (GBS)
INMARSAT
WGS
UFO
Commercial Ku Band
GPS
RQ4
MQ9
Harfng
JSTARS
Mission Network
Intel Network
Link 16
JFACC/A2
CJFHQ/J2
MCC/J2
Surface Combatants
SSN
LEGEND
Critical Requirement
Supporting System
Functional Relationship
Space System
Air System
Land System
Cyber Net
Communications (COM)
Positioning, Navigation, and Timing (PNT)
Remote Sensing (RS)
Information Management (IM)
GPS – Global Positioning System
CJFHQ – Coalition Joint Force Headquarters
JFACC – Joint Force Air Component Command (HQ)
MCC – Maritime Component Command (HQ)
SSN – Submersible Ship, Nuclear (Attack Submarine)
UFO – UHF Follow On
WGS – Wideband Global SATCOM

Figure 21: The "Knowledge Map" for the Intelligence Function

2.4 Module 2 Step 4 – Analysis of the ID Dependencies

The staff then executes the analysis of the ID relationships for each system. This leads to the determination of the enabling relationships, from which the ID dependencies are identified.

For example, the analysis of the ID relationships of the RQ4 may be summarized as follows
Communications: LOS considered unavailable in the context of the engagement; Regarding SATCOM providing BLOS communications capabilities:

- UHF MILSATCOMs (UHF Follow-on or Mobile User Objective System): failure would immediately degrade C2 data transmission: therefore, it is categorized as an enabler.
- Global Broadcast System (GBS)-related commercial Ku-band SATCOM: its failure would degrade C2 data transmission and immediately and continuously deny the dissemination of all ISR-collected data (SAR, Imagery, Full Motion Video) and would thereby degrade dynamic targeting as well as situational awareness; it is therefore categorized as an enabler.
- INMARSAT: used as backup relay for C2 data, its failure would have no disruptive effect on RQ4 ops; it is therefore categorized as an enhancer.

PNT: GPS is the main PNT system but is supplemented by inertial navigation system. Its failure would degrade the positioning of the vehicle over adversary-controlled area. It is therefore an enabler of RQ4

Conclusion: in the context of the engagement RQ4 is dependent on GPS for PNT and on commercial Ku-Band to disseminate ISR data.

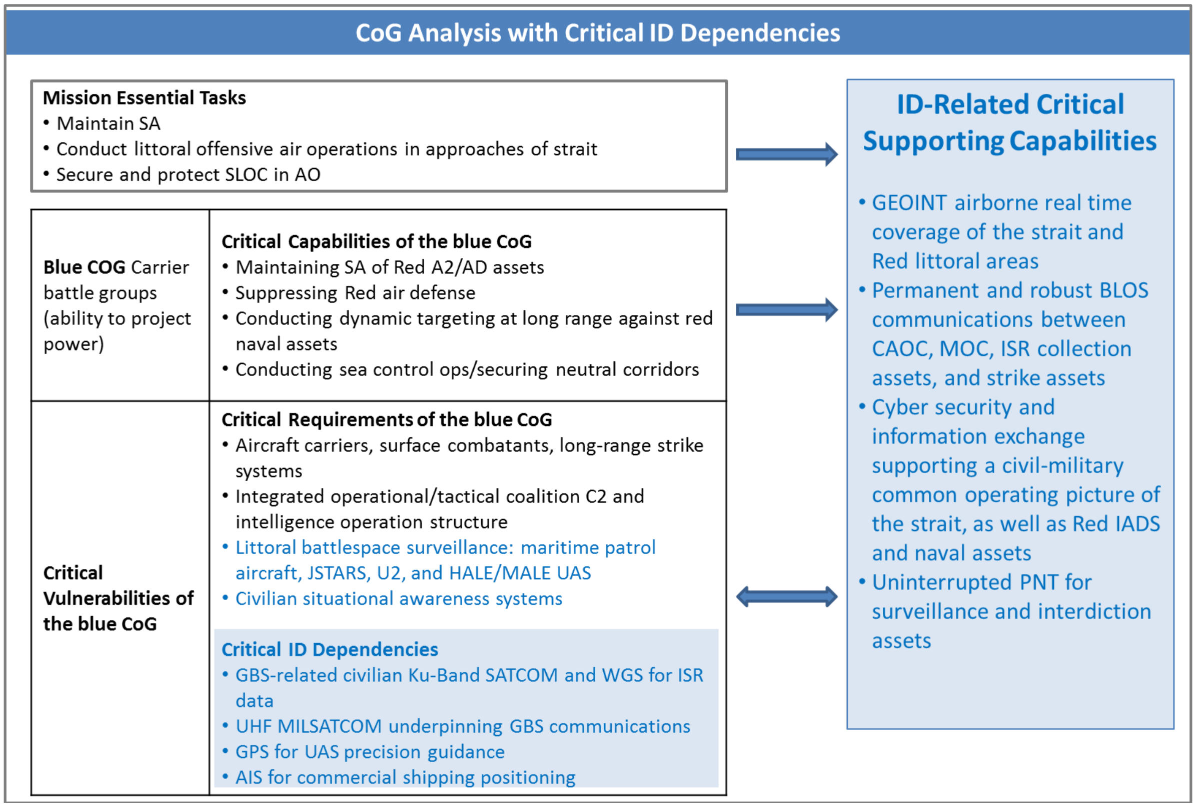
At the end of this analysis, other ID dependencies include:

- For French UAS: the EUTELSAT SATCOM system, since the anti-access environment limits the ability to conduct C2 and transmit the full motion video (FMV) from the UAS;
- For other American sensors: the GBS-related MILSATCOM systems, particularly the Wideband Global SATCOM, to disseminate the collected intelligence data to naval assets and to command and intelligence nodes;
- For the sea-launched cruise missiles, the GPS and the UHF SATCOM systems for guided munitions navigation and C2 communications.

Analyzing these dependencies, the staff identifies the critical ID dependencies for each MET:

- Regarding the MET "maintain SA"
    - The GPS for positioning/navigation of the airborne GEOINT sensors;
    - The GBS-related Ku-Band commercial and Wideband Global SATCOM systems to relay ISR data;
    - As commercial traffic resumes, AIS for commercial ships positioning.
- Regarding the MET to "secure and protect sea lines of communication", the staff identifies one main critical ID dependency:
    - The UHF MILSATCOMs underpinning CBG communications.
- Regarding the MET to "conduct offensive air operations", the staff considers the following critical ID dependencies:
    - MILSATCOMs critical to the secured relay of ISR C2 data and collected ELINT data;
    - GPS, for the precision guidance of cruise missiles and anti-radar missiles.

These critical ID dependencies are added to the list of CoG critical requirements.



CoG Analysis with Critical ID Dependencies

Mission Essential Tasks
- Maintain SA
- Conduct littoral offensive air operations in approaches of strait
- Secure and protect SLOC in AO

Blue COG Carrier battle groups (ability to project power)

Critical Capabilities of the blue CoG
- Maintaining SA of Red A2/AD assets
- Suppressing Red air defense
- Conducting dynamic targeting at long range against red naval assets
- Conducting sea control ops/securing neutral corridors

Critical Vulnerabilities of the blue CoG

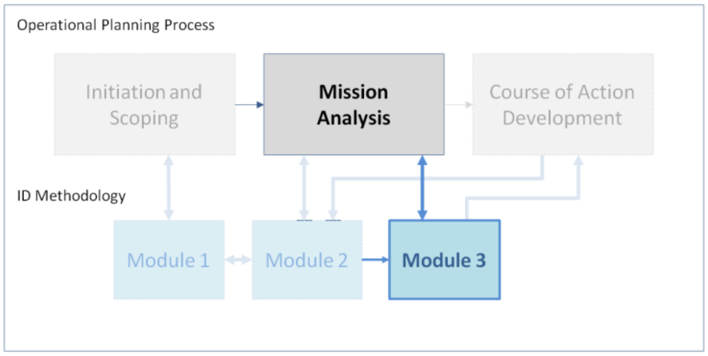
Critical Requirements of the blue CoG
- Aircraft carriers, surface combatants, long-range strike systems
- Integrated operational/tactical coalition C2 and intelligence operation structure
- Littoral battlespace surveillance: maritime patrol aircraft, JSTARS, U2, and HALE/MALE UAS
- Civilian situational awareness systems

Critical ID Dependencies
- GBS-related civilian Ku-Band SATCOM and WGS for ISR data
- UHF MILSATCOM underpinning GBS communications
- GPS for UAS precision guidance
- AIS for commercial shipping positioning

ID-Related Critical Supporting Capabilities
- GEOINT airborne real time coverage of the strait and Red littoral areas
- Permanent and robust BLOS communications between CAOC, MOC, ISR collection assets, and strike assets
- Cyber security and information exchange supporting a civil-military common operating picture of the strait, as well as Red IADS and naval assets
- Uninterrupted PNT for surveillance and interdiction assets

Figure 22 - CoG Analysis Including Critical ID Dependencies

4. Critical ID Vulnerabilities Identification (Module 3) – as Contribution to Mission Analysis



An input into module 3 would be the threats and hazards identified in the POE. In this example, as part of the POE, the J2 describes Red's counter-space and CNO capabilities and related vulnerabilities:

- ***Counter-space****;*
  - *Suspected powerful GPS jamming capability, available through an emerging power friendly to Red. Its employment is virtually certain in the event of armed confrontation. The GPS signal is therefore more vulnerable at shorter distances from the jammers. Red can reach the same effect by using CNO to degrade the GPS system.*

- *Mobile or fixed SATCOM jamming systems could affect Ku or C band satellite links.*
- ***Computer Network Operations***
    - *While unable to penetrate well protected networks, Red has demonstrated denial of service (DOS) capabilities, as well as an "advanced persistent threat" in the form of specific malware propagated in various protected systems linked to the Internet. The J2 assesses Red to be almost certain to employ these capabilities. Although the precise targets of such activities cannot be assessed, one of the C2 UAS links on commercial SATCOM is vulnerable to such activities because of recent network attacks on the control center.*
    - *Computer Network Intelligence (CNI) operations will be an important cornerstone in Red's courses of action because of Blue superiority to counter Red Computer Network Attack (CNA). Red will use CNI to gain understanding of Blue operations and methods. This understanding will then be used to design CNA where it has the most effect, to reach Red's desired effects.*
    - *Red can use CNO to degrade the GPS system.*
    - *Red will also use the Cyber ID for influence action toward various target audiences.*
    - *Red may also CNO to spoof AIS signal in the strait to usurp commercial ships positions and confuse coalition situational awareness in support of either concealment of Red ships or deception of coalition patrolling activities.*

The POE pointed out three vulnerabilities:

- *The GPS either to jamming or to CNO*
- *A commercial Ku-Band SATCOM system of the GBS*
- *The AIS spoofing through CNO*

2.5 Module 3 Step 1- Analysis of the Critical Vulnerabilities Stemming from Each Threat/Hazard

The possible chains of effects stemming from these vulnerabilities are developed and show that:

- **GPS vulnerability to jamming/CNO** would hamper the provision of PNT data over the area of operations (direct effect), thereby providing Red with an area-denial rather than anti-access capability. More specifically, it could cause the following chain of indirect effects:
    - It would hamper the navigation of some attack aircraft, degrading the use of air-launched PGMs as well as the use of sea-launched cruise missiles, narrowing the weaponeering options for strikes, thereby disrupting capabilities related to the fires function.
    - It would degrade the time-synchronization of the communications on the Link-16 network leading to a degradation of the networking between sensors, CAOC and shooters. It would preclude the use of MALE UASs and other air sensors over the area, thereby degrading the capabilities of GEOINT real-time surveillance.
    - It would deny the execution of SEAD targeting of mobile components of IADS.
    - It could degrade the C2 capabilities for naval command ships requiring GPS for PNT.

  The GPS vulnerability is assessed as a critical ID vulnerability for both CoG critical capabilities to execute long-range dynamic targeting against red naval assets and to execute dynamic SEAD and thereby to both METs “conduct offensive air operations” and “secure and protect sea lines of communication”.

- **Civilian Ku-band SATCOM vulnerability** to the highest level of computer network attack by Red would result in the direct effect of a risk of spoofing of the Global Hawk C2 data. The indirect effects of this would be the potential hijacking of UAV, which would thereby degrade the capability to maintain a GEOINT real-time surveillance and, beyond that, create a severe blow to the coalition morale. The vulnerability of GBS’s civilian SATCOM but also, indirectly, the vulnerability of the Global Hawk itself, which is dependent on this system for its C2 data transmission, are assessed as critical ID vulnerabilities for the METs “establish and maintain situational awareness” and “conduct offensive air operations”, for which the naval force requires near-real time ISR data but less for the MET “Secure and protect sea lines of communication”, whose critical requirements rely less on this specific asset.

- **The AIS vulnerability to spoofing** would enable Red to exploit the AIS to disseminate false positioning and navigation information of the commercial ships (direct effect). Indirect effects intended by Red would be the concealment of Red naval assets and/or the deception of coalition naval activities in the strait. Another indirect effect would be the degradation of trust in the common operating picture, leading to a degradation of the situational awareness of the maritime domain. The mitigation measure would be to reinforce the cross-cueing of information with ISR sensor data, placing an additional burden on these limited resources.

2.6 Module 3 Step 2 – Refinement of the Critical ID Vulnerabilities

The correlation of the three chains of effects is undertaken. For example:

- **For the MET “conduct offensive air operations”** (see illustration below): the correlation of GPS jamming which would degrade all sensors over the area and spoofing of the GBS SATCOM civilian system, which could result in the hijacking of the RQ4 Global Hawk, would lead to severe degradation of the capability to provide GEOINT real-time surveillance. This would leave the force reliant on space assets and stand-off SIGINT surveillance systems. Combined with the effect of the GPS jamming on the ability to guide long-range weapons, and the effects on the C2, the main outcome would be the denial of the ability to execute dynamic targeting of Red naval assets. Concurrently, the GPS vulnerability would affect the situational awareness of the Red IADS in a more limited manner due to remaining stand-off ELINT capabilities, but would nullify the capability to suppress these IADS assets. The combination of both chains of indirect effects would thereby narrow options to perform the MET. The commander would need to rely on deliberate targeting and the use of other weapons (laser guided weapons for example) with limited freedom of maneuver due to IADS. Mitigation options could include:
    - Reliance on manned platforms, such as P3, less dependent on the vulnerable GPS signal and not relying on commercial Ku-Band SATCOM;
    - Reliance on more naval SIGINT platforms such as the SNA;
    - The development of a COA less reliant on the dynamic targeting of Red naval and IADS assets.

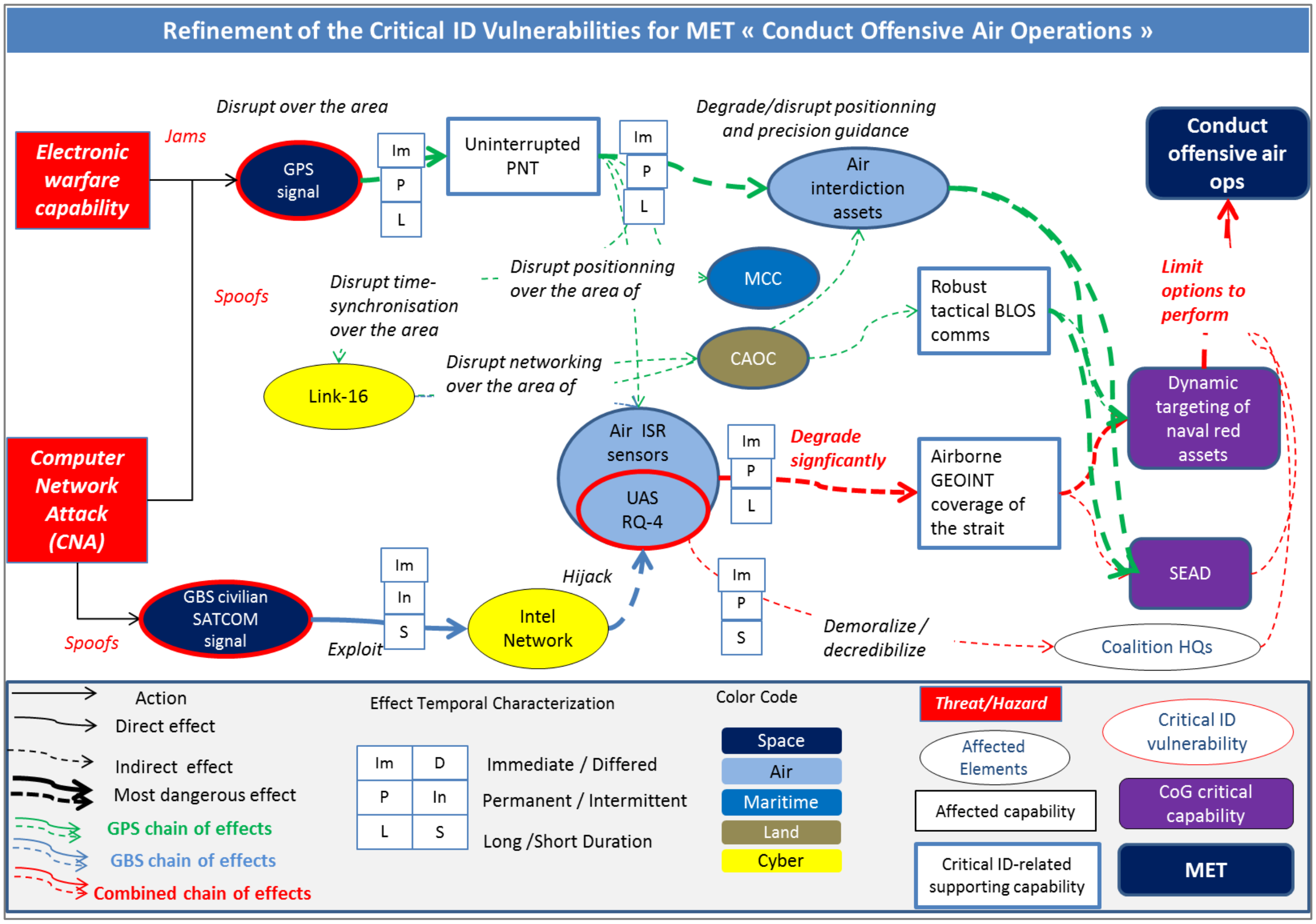
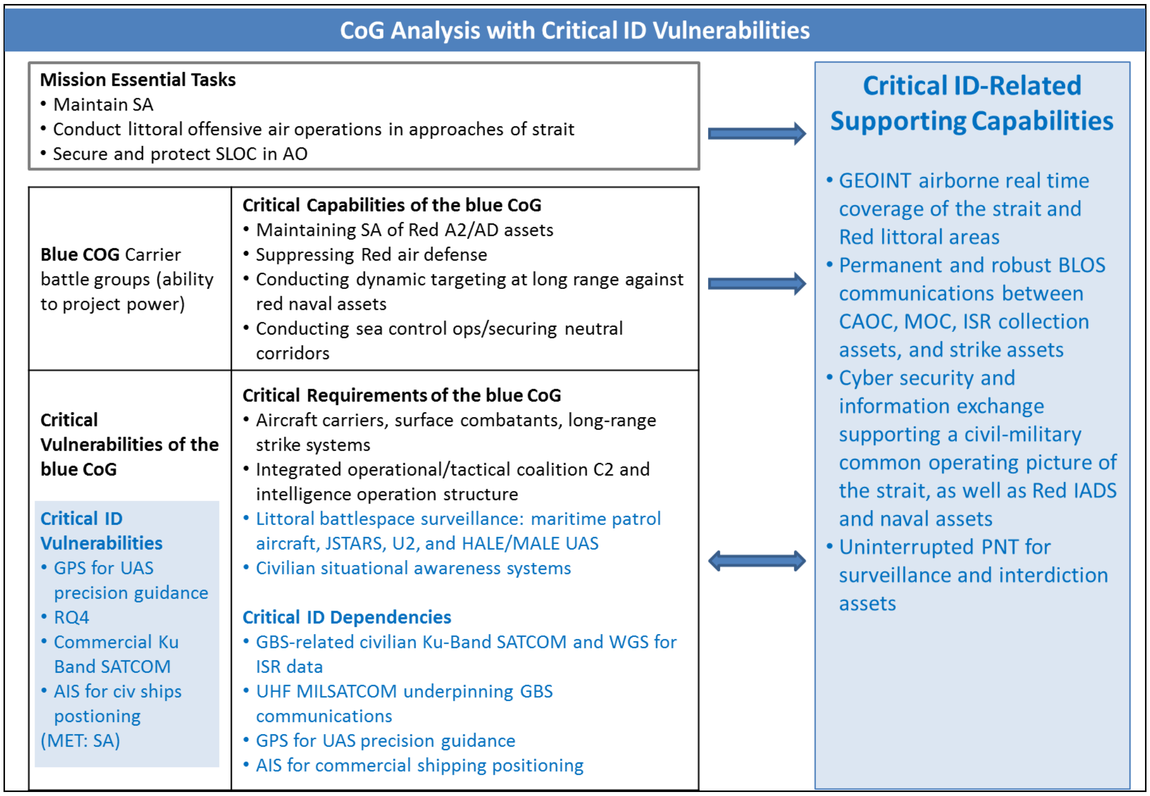

Refinement of the Critical ID Vulnerabilities for MET « Conduct Offensive Air Operations »
Electronic warfare capability
Jams
Disrupt over the area
GPS signal
Im
P
L
Uninterrupted PNT
Im
P
L
Degrade/disrupt positionning and precision guidance
Air interdiction assets
Conduct offensive air ops
Spoofs
Disrupt time-synchronisation over the area
Disrupt positionning over the area of
MCC
Robust tactical BLOS comms
Limit options to perform
CAOC
Link-16
Disrupt networking over the area of
Dynamic targeting of naval red assets
Computer Network Attack (CNA)
Air ISR sensors
UAS RQ-4
Im
P
L
Degrade signficantly
Airborne GEOINT coverage of the strait
SEAD
Im
In
S
Hijack
Im
P
S
GBS civilian SATCOM signal
Spoofs
Exploit
Intel Network
Demoralize / decredibilize
Coalition HQs
Action
Direct effect
Indirect effect
Most dangerous effect
GPS chain of effects
GBS chain of effects
Combined chain of effects
Effect Temporal Characterization
Im
D
Immediate / Differed
P
In
Permanent / Intermittent
L
S
Long /Short Duration
Color Code
Space
Air
Maritime
Land
Cyber
Threat/Hazard
Affected Elements
Affected capability
Critical ID-related supporting capability
Critical ID vulnerability
CoG critical capability
MET

Figure 23: Potential Indirect Effects of GPS and GBS Vulnerabilities for Mission Essential Task "Conduct Offensive Air Operations"

- **Regarding the MET "maintain situational awareness"**, the combination of threats on GPS, on the Global Hawk through the vulnerable commercial Ku-Band SATCOM, and on AIS would cause a severe degradation of the ability to establish a near-real time common operating picture and thereby to execute this MET. The additional ISR sensors required to offset degraded situational awareness of the commercial shipping stemming from the spoofing of AIS, would be degraded due to the spoofing of the GPS signal. The mitigation option would be to rely more on space assets and other less capable (in terms of coverage) naval and air sensors to maintain a degraded common operating picture.



CoG Analysis with Critical ID Vulnerabilities

Mission Essential Tasks
- Maintain SA
- Conduct littoral offensive air operations in approaches of strait
- Secure and protect SLOC in AO

Blue COG Carrier battle groups (ability to project power)

Critical Capabilities of the blue CoG
- Maintaining SA of Red A2/AD assets
- Suppressing Red air defense
- Conducting dynamic targeting at long range against red naval assets
- Conducting sea control ops/securing neutral corridors

Critical Vulnerabilities of the blue CoG

Critical ID Vulnerabilities
- GPS for UAS precision guidance
- RQ4
- Commercial Ku Band SATCOM
- AIS for civ ships postioning

(MET: SA)

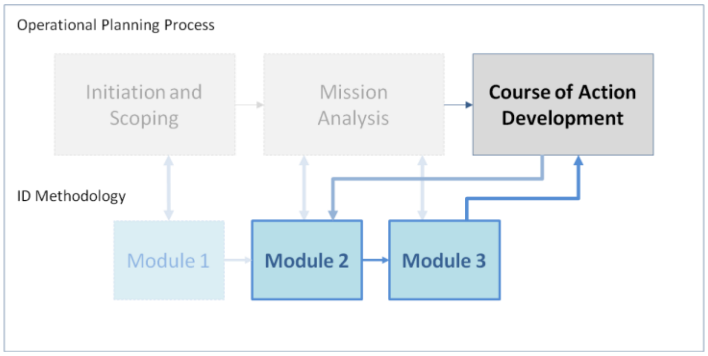
Critical Requirements of the blue CoG
- Aircraft carriers, surface combatants, long-range strike systems
- Integrated operational/tactical coalition C2 and intelligence operation structure
- Littoral battlespace surveillance: maritime patrol aircraft, JSTARS, U2, and HALE/MALE UAS
- Civilian situational awareness systems

Critical ID Dependencies
- GBS-related civilian Ku-Band SATCOM and WGS for ISR data
- UHF MILSATCOM underpinning GBS communications
- GPS for UAS precision guidance
- AIS for commercial shipping positioning

Critical ID-Related Supporting Capabilities
- GEOINT airborne real time coverage of the strait and Red littoral areas
- Permanent and robust BLOS communications between CAOC, MOC, ISR collection assets, and strike assets
- Cyber security and information exchange supporting a civil-military common operating picture of the strait, as well as Red IADS and naval assets
- Uninterrupted PNT for surveillance and interdiction assets

Figure 24 - CoG Analysis Including Critical ID Vulnerabilities

5. Methodology Contribution to COA Development



The J2 considers two ECOAs, based partially on the critical ID vulnerabilities previously identified:

- A most probable COA aiming to undermine the credibility of the coalition force could combine:
  - Selective GPS jamming to create collateral damage as soon as Blue interdiction assets start to deliver weapons;
  - Selective CNA to capture/destroy one UAS and exploit it in the media;
  - Deployment of air and naval assets across/above the Strait to highlight the continuous ability of Red forces to patrol the strait despite coalition presence;

  - Concealment, camouflage and deception (CCD) measures, through the spoofing of AIS signals, to increase the efficiency of Red naval assets operations;
- A most dangerous COA aiming to deny the ability to re-establish FoN in the Strait based on:
  - The combination of full-range and aggressive of EW- CNA operations, air defense against Blue air forces to deny the ISR and offensive air operations;
  - Attacks on all coalition naval assets entering into the Strait.

During the initiation and scoping and mission analysis, the commander and his staff developed an operational design articulated as follows:

- *A first short phase aiming to forcefully reopen the strait by obtaining air superiority and destroying most of the Red assets which deny the access to the strait;*
- *A second longer phase aiming to ensure and maintain access to and FoN in the strait by destroying residual Red capabilities and escorting commercial traffic as it resumes.*

Based on this operational design, the staff develops two COAs:

- *A "rolling back" COA in which coalition forces intend to suppress Red anti-access then area denial capabilities then to protect the resuming traffic. It envisions:*
  - *A first active phase to seize the initiative, by degrading in depth Red anti-access air and naval forces with long range airpower and submarine forces;*
  - *A second phase to decisively dominate Red's naval area denial forces and re-open the strait, relying primarily on carrier battle groups CBGs;*
  - *A third phase to reopen the strait and escort commercial ships.*

  The staff updates functional Kmaps of ID dependencies and influence diagrams of critical ID vulnerabilities throughout these phases. It concludes that while the critical ID dependencies would remain, the relative criticality of the GBS would diminish as more "tactical" sensors, strikes assets and C2 nodes would operate closer in, relying on their line of sight tactical data links and therefore making their need for the Global Hawk less pressing. Conversely, as more assets would operate in the area close to Red, the assets representing critical ID vulnerabilities stemming from the "limited" GPS disruption would expand dramatically. While the AIS would be a limited issue for the two first phases of this COA, it would clearly become a critical vulnerability as the commercial traffic resumes.

- *An "Ink spot" COA relying on Green state support, that envisions more parallel offensive and defensive operations. It is articulated as follows:*
  - *A first offensive phase to seize the initiative, while securing basing options for airpower in Green states;*
  - *A second phase to reopen and secure a local maritime corridor near Green states coasts as soon as possible, to escort resuming commercial traffic, while executing relentless offensive operations against Red naval assets, relying on naval CBGs and as a branch, airpower based on Green states;*
  - *The third phase to continue the escort commercial ships until Red is compelled to give up its claim.*

This type of COA would mitigate risks associated with the overreliance on BLOS communications for UAS, notably the Global Hawk. By operating through LOS datalink, it would no longer be a critical vulnerability. Conversely, the vulnerability represented by the AIS could become more critical as it could potentially hinder both offensive and defensive operations against Red naval assets.

Intentionally Blank

Appendix B: The ID Functional Models

1. Introduction

1.1 Purpose

The purpose of the ID functional models is to provide an overall perspective of the possible inter-domain relationships between capabilities related to the different military functions or non-military domain functions. The ID functional models are generic, reflecting the fact that a number of standing inter-domain relationships between systems and elements remain unchanged regardless of the context; they are not related to a specific set of capabilities or to a specific situation.

During planning, they are used as an intellectual tool to facilitate the identification and categorization of capabilities and systems, and their related inter-domain relationships, for a given military function or non-military domain function. They therefore support the application of modules 2 and 3 of the methodology described in this guide.

1.2 Content

ID functional models are based on a representation of the capabilities related to military functions or non-military domain functions, focusing on space and cyber capabilities. The representation also includes the systems and system elements [or sub systems] that contribute to a given capability as well as the ID relationships that functionally link these systems and sub systems together.

They include:

- A graphical depiction of the linkages among functions, primary and supporting capabilities, and related systems;
- A narrative providing a short explanation of the types and characteristics of inter-domain relationships that could exist among capabilities or activities to perform the given military function or a non-military domain function.

Ultimately, ID functional models should be developed:

- For each military function:
  - Command and control
  - Intelligence
  - Fires
  - Movement and maneuver
  - Force protection
  - Sustainment
- For the non-military domain functions:
  - Maritime domain access and operations

- ○ Air domain access and operations
- ○ Space domain access and operations
- ○ Cyber access and operations

Two examples of ID functional models, related to the Intelligence function and to the C2 function are provided below.

2. ID Intelligence Functional Model

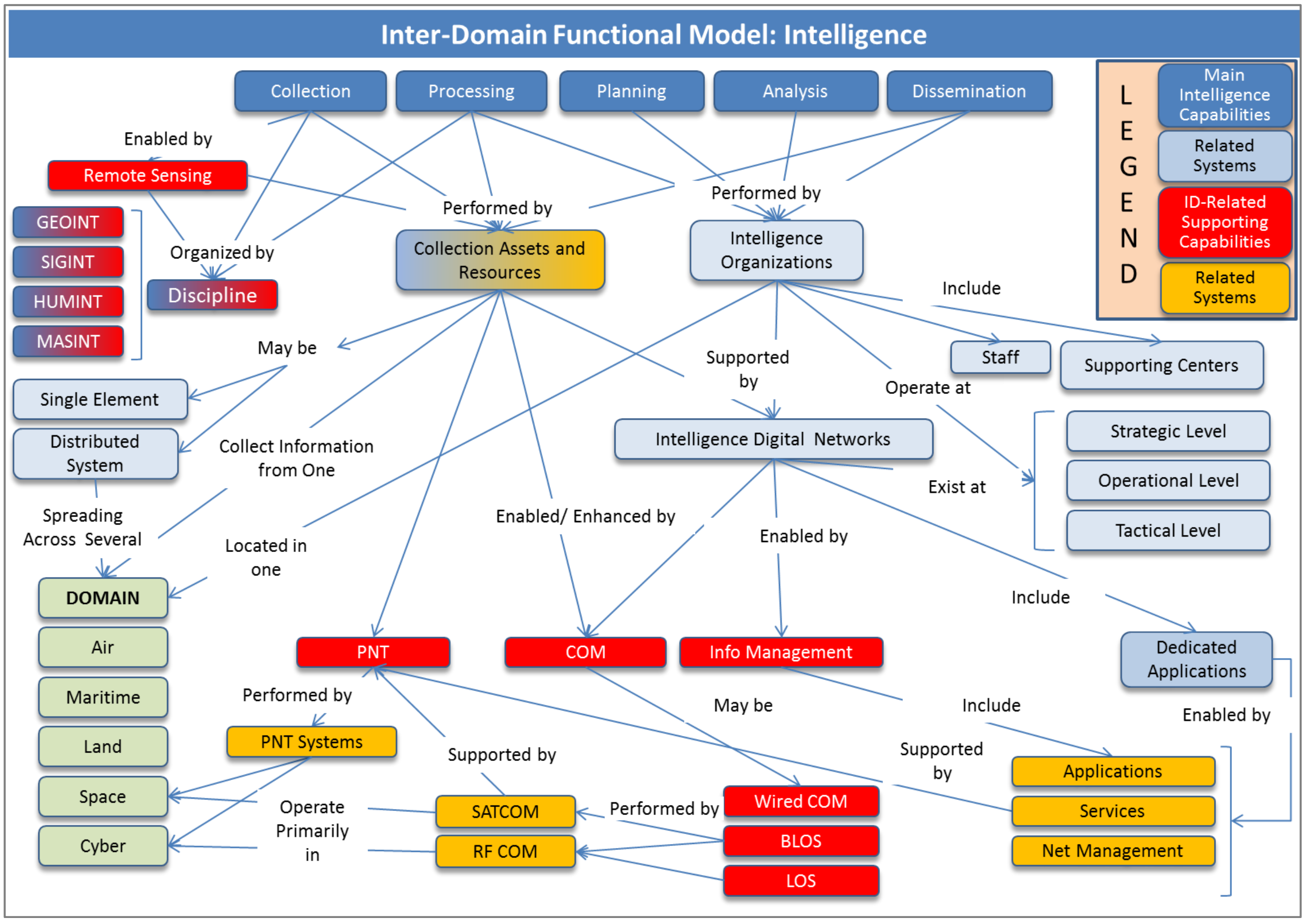


Figure 25 – Representation of an ID Intelligence Functional Model

2.1 Introduction

This ID functional model exposes the inter-domain dimension of capabilities enabling the intelligence function of a military force[25].

[25] It is based on a conceptual framework developed in the MNE7 Outcome 4 Conceptual and Pre-Doctrinal Paper: Understanding Inter-Domain Dependencies and Vulnerabilities, dated November 29, 2012. Elements of this conceptual framework are reflected in Appendix D "Key Terms".

This model is articulated along several categories:

- The main capabilities needed for the intelligence function and the systems related to these primary capabilities;
- The ID-related supporting capabilities and the systems related to these ID-related supporting capabilities.

This model focuses on the capabilities provided by systems operating primarily in the cyber and space domains.

2.2 Primary Intelligence Capabilities and Related Systems

For the intelligence function, the **main capabilities** are the sub-functions of the intelligence process:

- Planning
- Collection
- Processing
- Analysis
- Dissemination.

These primary capabilities, which in this case include “remote sensing” capabilities, are provided by the following systems and assets:

- The intelligence organizations have the following characteristics
  - They include staffs and supporting processing and analysis centers
  - They may
    - Plan intelligence and collection requirements
    - Process and disseminate intelligence in one or more disciplines:
      - Geo- intelligence (GEOINT)
      - Signals Intelligence (SIGINT)
      - Measurement and Signature Intelligence (MASINT)
      - Human Intelligence (HUMINT)
    - analyze and disseminate all-source intelligence products and
  - They may operate at the strategic, operational and tactical level, and
  - They may be located in different domains.

- The collection assets and resources, have the following characteristics
  - They collect information primarily from one domain,
  - They are composed either of a single sensor element (for example a ship), or of an inter-domain system distributed in different domains (UAS for example)
  - They collect information in one or more disciplines:
    - Geo-intelligence (GEOINT)
    - Signals Intelligence (SIGINT)
    - Measurement and Signature Intelligence (MASINT)
    - Human Intelligence (HUMINT)
  - They include

        - The force's collection assets and other collection resources which are dedicated to the intelligence function or
        - Other collection resources of the force which are non-dedicated to the intelligence function.

- The intelligence networks which connect and support the intelligence organizations and the collection assets and may exist at the strategic, operational and tactical level. The intelligence networks include set of applications dedicated to the primary capabilities.

2.3 ID-Related Supporting Capabilities, Related Systems and their Relationships

The intelligence networks and ISR systems are enabled by three supporting capabilities: information-management capabilities, communications capabilities and PNT capabilities. These capabilities and supporting systems are described below.

- **The Intelligence networks** are enabled by:

    - Information management capabilities in the cyber domain, which include
        - the set of functional applications;
        - network management;
        - the provision of enterprise services;
        - information assurance.
    - Communications capabilities, including
        - Switching and routing capabilities;
        - Wired-communications capabilities for long haul information transport between fixed intelligence organizations and with fixed elements of the collection systems;
        - beyond Line of Sight (BLOS) communications, mainly provided by SATCOM systems
            - EHF/Ka Band secure SATCOM systems for secured, jam-resistant, low data rate communications;
            - SHF/Ku Band SATCOM, either military and civilian, medium to high data rate, to broadcast GEOINT product;
            - UHF/S-Band/C-Band SATCOM for low data rate communications with mobile systems
        - Line of Sight (LOS) communications provided by other UHF RF communications;
    - PNT capabilities which enable the enterprise services of the network.

- **The airborne collection assets and resources** are enabled/enhanced by:

    - Information management capabilities, mainly
    - Communications capabilities allowing the transmission of C2 data of the collection system and collected data
        - between the elements of the system (platform and control element)
        - between the system and intelligence organizations, such as processing centers and intelligence staffs

      GEOINT and video transmissions are the most demanding in terms of bandwidth and require use of SHF Ku-Band. The communications capabilities include
        - Wired-communication capabilities between fixed elements of collection system;

        - Beyond Line of sight capabilities, the SATCOM systems;
        - Line of sight capabilities, by other RF COM systems.

    - PNT capabilities necessary for the positioning, the navigation, for the timing synchronization of the radar systems, which may be provided by:
        - The space PNT mainly provided by GPS, and in the near future by Galileo;
        - Radio systems enabling positioning and navigation, notably the LORAN and eLORAN system.

- **The naval collection assets and resources** are enabled/enhanced by:

    - Communications capabilities allowing the transmission of C2 data of the collection system and collected ISR data between the naval platform and users. Imagery and video transmissions are the most demanding in terms of bandwidth and require use of SHF Ku-Band. In the case of naval collection systems, these capabilities (mainly Beyond Line of Sight) are provided by the SATCOM.
    - PNT capabilities necessary for the positioning, the navigation, for the timing synchronization of the radar systems, which may be provided by:
        - The space PNT mainly provided by GPS, and in the near future by Galileo,
        - The PNT radio, notably the LORAN and eLORAN system.

- **The space-based collection assets and resources** are enabled/enhanced by:

    - Wired-communications capabilities between elements of the control segment of the system,
    - PNT capabilities that are necessary to control the spacecraft and the signal, and may be provided by the space PNT systems (mainly the GPS, in the near future by Galileo).

ISR assets and resources provide both the intelligence function's collection capability and the bulk of remote sensing, which is considered here to be an ID-related supporting capability. Although most surveillance and reconnaissance systems were once primarily intended to feed intelligence analysis (as collection assets and resources), in network enabled operations they are also providing remote sensing capability in direct support of the C2, Fires and Protection functions. However, given that these ISR assets and resources are discussed in the context of the collection capabilities of the intelligence function, to avoid repetition they are not addressed a second time specifically with regard to remote sensing. Nevertheless, some ISR collection resources are not related to remote sensing (for example, all direct observation means), and some remote sensing assets are not intelligence-related even though the information they acquired could be exploited later for intelligence purposes. The latter include but are not limited to:

- Early warning systems;
- Battle management systems (providing RADINT/ Ground Moving Target Indications or Full-Motion Video);
- Weapon systems sensors (dubbed as "non-traditional ISR");
- Weather systems.

3. ID Command and Control Functional Model

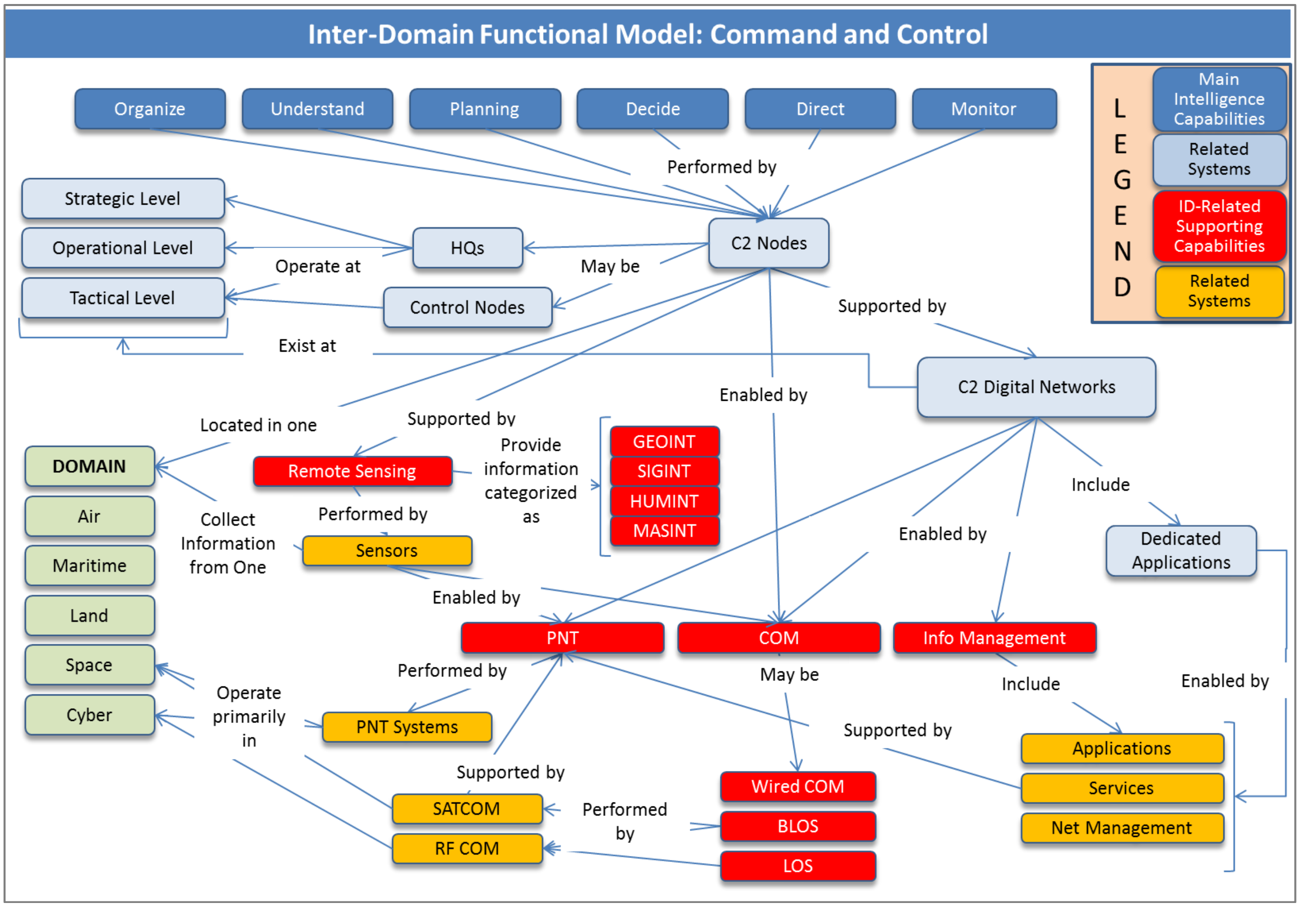


Figure 26 - ID Command and Control Functional Model

3.1 Introduction

This functional model exposes the inter-domain dimension of capabilities that enable a military force's command and control function.

This model is articulated along several categories:

- The primary capabilities needed for the C2 function and the systems related to these primary capabilities;
- The ID-related supporting capabilities and the systems related to these ID-related supporting capabilities.

It focuses on the capabilities provided by systems operating primarily in the cyber and space domains.

3.2 Primary Capabilities and Related Systems

It is assumed that command and control activities rely notably on information communication, processing and sharing as well as positioning, navigation and timing capabilities

As a reminder, the **main capabilities** ensuring command and control are:

- Organize
- Understand
- Planning
- Decide
- Direct
- Monitor[26].

These capabilities are provided by C2 nodes and C2 networks.

- **C2 nodes** may be
  - Headquarters operating at the strategic, operational and tactical level, generally located in the land and maritime domains;
  - Control nodes (for example, an AWACS) operating at the tactical level connecting combat and supporting assets.
- These C2 nodes are supported by **C2 networks**, which may exist at the strategic, operational and tactical level (i.e. Link-16 networks). C2 networks include set of applications dedicated to the command and control capabilities.

3.3 ID-Related Supporting Capabilities, Related Systems and their Relationships

These main C2 capabilities and the associated C2 nodes and supporting networks are enabled by communications, PNT and information management capabilities.

- C2 networks rely on **Information management capabilities** in the cyber domain, which include
  - The set of applications
  - The provision of enterprise services which directly enable the dedicated applications
  - The management of the network, and
  - Information assurance;

- C2 networks, and C2 nodes on their own, are critically enabled by **communications capabilities** which provide the physical layers of such networks.
  - Wired-communications capabilities enable networks of fixed C2 nodes at strategic, operational and tactical level. These capabilities may be linked to Internet;
  - Beyond Line of Sight (BLOS) communications capabilities enable deployable operational networks, reach-back to strategic nodes and increasingly tactical networks. They are mainly provided by SATCOM systems
    - EHF/Ka Band secure SATCOM systems for secured, jam-resistant, low to medium data rate communications;
    - SHF/Ku Band/C Band/X Band SATCOM, medium to high data rate, to broadcast imagery and video;
    - UHF/S-Band SATCOM for low data rate communications with mobile systems;

    These SATCOM are either controlled military assets or leased from commercial firms.

[26] See US Joint Staff/J7, Joint Capabilities Areas Framework, http://www.dtic.mil/futurejointwarfare/strategic/jca_framework.xls

The capabilities may also be provided by airborne relay systems such as UAS.

  - Line of sight UHF communications capabilities enable traditionally tactical networks.

- C2 networks, and C2 nodes on their own, are enabled **Positioning Navigation and Timing capabilities**
  - To perform understand and monitor capabilities, networks are supported by Positioning and navigation capabilities for the development of the common operating picture, more specifically to permanently update the positioning of controlled units and known threats and relevant elements of the operational environment.
    - PN capabilities may be supported by UHF SATCOM systems;
      - Timing capabilities may enable SATCOM and RFCOM communications systems using Time Division Multiple Access by allowing the synchronization of the data transmission;
      - PNT are mainly provided
    - By space systems, GPS, in the near future by Galileo
    - By the PN radio systems, notably the LORAN and eLORAN system.

- C2 nodes are supported by **remote sensing capabilities**
  - To support the “understand” and “monitor” primary capabilities, C2 nodes require combat and support information, mainly through the GEOINT, SIGINT, MASINT disciplines. This information includes early warning, battle management (notably Full Motion Video, Ground Moving Target Indications) and other supporting information such as weather information. This information is potentially provided by the full range of surveillance and reconnaissance systems, notably by space systems, unmanned and manned air, naval and ground platforms or distributed ID systems, as well as weapon system sensors. Although most surveillance and reconnaissance systems were once primarily intended to feed intelligence analysis (see collection assets and resources in the intelligence function model), in network enabled operations they are also providing remote sensing capability in direct support of the C2, Fires and Protection functions.
  - Remote sensing capabilities are themselves enabled by PNT, COM and information management capabilities.

Appendix C: Requirements for Tools

1. Introduction

Although tools are not required to apply the methodology, some tools may nonetheless greatly facilitate its implementation by saving time during the decision-making process.
The tools discussed here are the following:

- A systems database and associated systems operational views;
- A tool to facilitate the development of the Kmaps;
- Ontology tools.

2. Development of a systems database and associated systems operational views

2.1 Purpose

The methodology in particular imagines the development of an "ID systems database" and a tool that would enable the conversion of the elements within the database into systems operational views. The purpose of these would be to capture and support the visualization of the inter-domain relationships among key systems or assets.

These could be proposed and populated in advance during peacetime by each interested nation, based on existing data, such as data generated in the technical documentation of a given system in the course of its development and operational life. Indeed, although the nature and level of inter-domain dependencies is generally context-dependent, nonetheless, a number of standing inter-domain relationships between systems and elements remain unchanged regardless of the context.

Once the databases and associated systems operational views had been established, they could be shared during the coalition planning process, according to the identified information exchange requirements[27]. By contributing to pre-identifying the standing systems or elements and their relationships, the database and systems operational views would support the mapping of the operation-specific ID relationships (Kmap development) and subsequent analysis of the ID dependencies during the planning process (module 2 of the methodology). They would provide analysts and planners with a solid basis from which to work when they undertake their modeling of the ID System for a specific operation.

[27] The guide recognizes that this type of database would likely be classified. Sharing the information in this type of database would therefore require specific information-sharing agreements.

2.2 Specification

The database should be based on two taxonomies, derived from the conceptual framework developed in the Conceptual and Pre-Doctrinal Paper and briefly addressed in appendix D of this guide. These taxonomies share the same upper level part, from “actor” to “system”.

- The first taxonomy considers each given system as one entity and is suited to generate the systems operational views (SOV) and Kmaps displaying the functional ID relationships between systems;
- The second considers the elements of a given system and is suited to generate the detailed SOVs which complement the SOVs and Kmaps by displaying the ID physical and functional relationships among the elements of the system and between these elements and supporting systems.

Used for SOVs and Kmaps	Used for detailed SOVs
Actor **Function** **Domain** **Capability** **System**	
ID-Related Supporting Capability **ID Functional Relationships** **Supporting Systems** **Supported Systems**	**System Element** **ID-Related Supporting Capability** **ID Relationship Functional Characteristics** **ID Relationship Physical Characteristics Attributes** **Supporting Systems (linked via the ID relationship)** **Supported Systems**

Table 5- ID Systems Database Taxonomy

A generic example of what this database could resemble and the corresponding detailed systems operational view is presented in the figure below.

ID Functional Model Level Data				Systems Operational View Level Data							
Actor	Function	Domain	(ID) Capability	System Type	System Name & Type	Element	ID related Supporting Capability	ID Relationship Functional Characteristics	ID Relationship Physical Characteristics	Supporting System(s) / Element	Supported System(s) / Elements
Coalition	Intel	Air	Collection	UAS, HALE	UAS X	Air Vehicle	BLOS com	DwnLink: Sensor data, vehicle status Uplink: C2 data	Ku band, Permanent, downlink while on station, 40 Mbps	SATCOM A	• Mission control element • Remote Intel exploitation centers in direct transmission
							BLOS com	Back-up C2 datalink Uplink: C2 Dwnlink: vehicle status	Permanent, UHF	SATCOM B	• Mission control element • Launch and recovery element
							LOS com	DwnLink: Sensor data, vehicle status Uplink: C2 data	Ku band, Permanent, while on station, 200 Mbps	Datalink E	• Mission control element • Remote Intel exploitation centers in direct transmission
							PNT	Positioning data	L band signals, receive only Updates only, low frequency,	GPS	
						Mission Control Element					
						Launch and Recovery Element					

Table 5: Example of Database Entry Regarding a HALE UAS

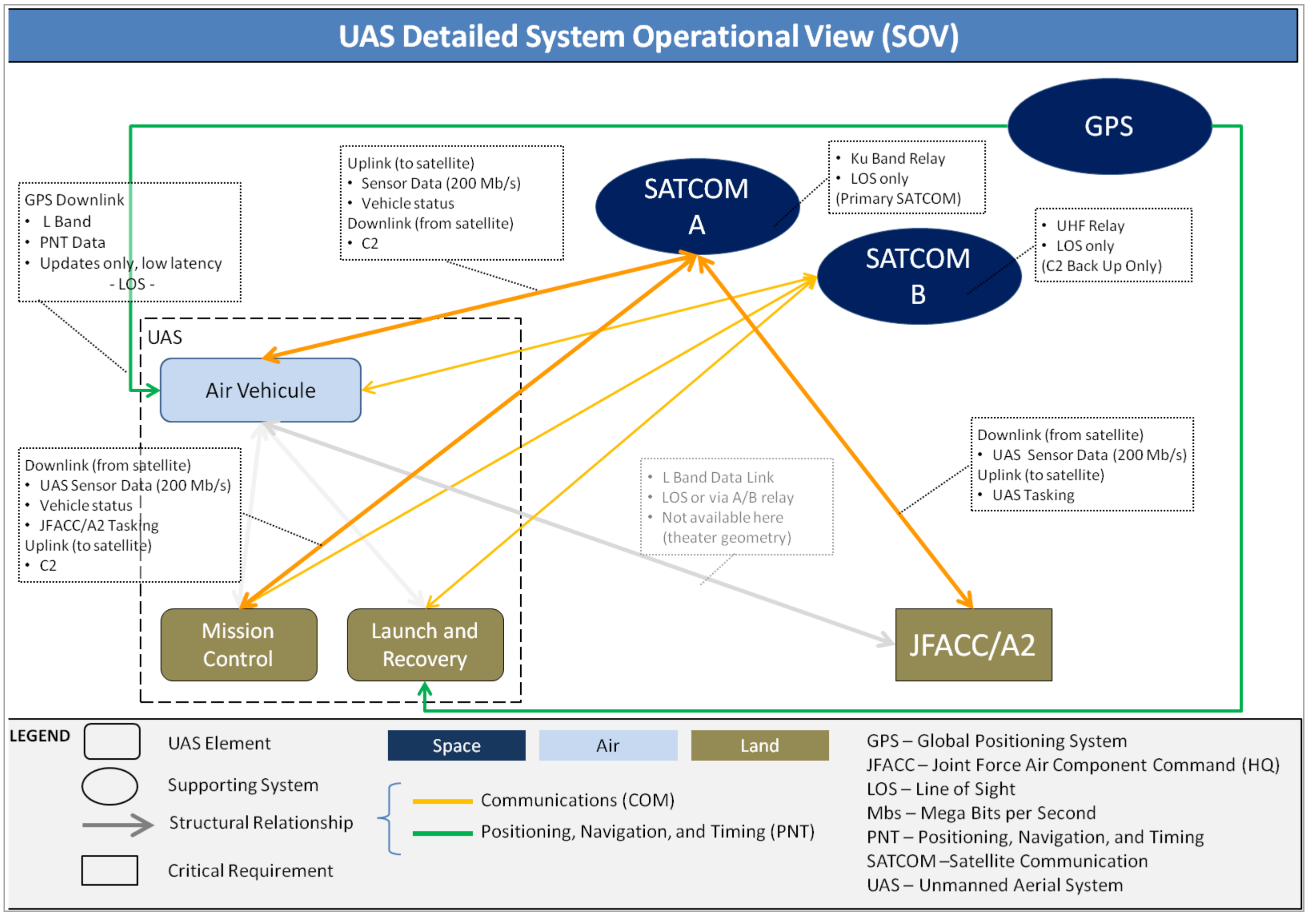


Figure 27: Detailed System Operational View of ID Supporting Relationships

3. Requirements for a Tool to Develop Kmaps

The database described above could also provide additional export features to automatically generate Kmaps, as specified in this guide (see page 37, "Mapping ID Relationships") based on:

- The operator selection of a list of systems to be displayed;
- Additional operator inputs regarding the supporting systems to be included (for example, if more than one supporting system can provide the required capability for a given system in the database) or other operation specific constraints (theater geometry, weather, etc.).

As stated in module 2, the methodology proposes the development of one Kmap per relevant military function and per considered non-military domain function. A computer tool – particularly one already linked to the systems database and operational views described above – would save a great deal of time in developing these Kmaps. Furthermore, the methodology proposes the interlinking of Kmaps to determine the cross-functional systems. For example, the analyst should be able to superimpose or switch from the C2 Kmap to the Intelligence Kmap when he or she works on the dependencies stemming from a given CWAN critical for both functions. Thus, a computer tool enabling the super-imposition of the various Kmaps would facilitate the analyst's work.

As stated pages 38-39 of this guide, the Systems Operational Views and Kmaps should include the following elements:

- Specific symbols/visualization for:
  - The ID System elements (systems, assets) providing the capabilities, distinguished by domains: space, cyber, air, maritime as well as the land domain where relevant;
  - The various types of relationships, e.g. supporting, enabling, enhancing;
  - The critical ID dependencies;
- Text box outlining relevant information regarding the considered element, relationships and dependencies. Ideally, the computer tool would enable the visualization of the relevant information by clicking on the element in order to zooming in.

A tool could also be used to support the development of the detailed SOVs in a similar manner.

4. Using an Ontology Tool

The key terms presented in appendix D, as well as the ID functional models, are built as ontologies.

An ontology is a semantic model that represents knowledge about a given topic. An ontology is composed of terms, sorted in classes (i.e. Actors, Capabilities, Systems, Elements) and semantic links (i.e. "Related to", "Have attribute") that describe the relationship between the terms. By using the semantic links to connect terms, axioms summarizing this knowledge can be built (i.e. "The system is composed of elements"). By checking the accuracy of those axioms, the coherence of the ontology can be examined.

Based on these general ontologies, as proposed in the conceptual framework (as described in the appendix D related to key terms[28]) and ID functional models (described in appendix B), various ontology tools could be used to model the ID System related to a given engagement and to incorporate the data related to it. The data provided would be the actual instances of the classes (i.e., the GPS, the UAS X) and linkages. In addition, "Reasoner" tools are able to infer what class a new element belongs to, based on the properties introduced by the analysts.

These tools could save the operator a great deal of work and can help to maintain the coherence of the database. For example, any time that an element is stated to be part of a System, the "Reasoner" will list that element in the list of elements composing the System. Any time that a system is stated to be composed of an element, the element will be marked as being part of that system. The tool enables the propagation of properties in both directions (i.e. "the UAS X is composed of the air vehicle element" and "the air vehicle is part of the UAS X"). The tool is able to infer additional linkages (i.e. the GPS has an enabling relationship with the UAS X air vehicle element → the GPS has an enabling relationship with the UAS X). If properly populated, the tool can therefore infer the chains of functional relationships between the various functions, systems and elements and support the analysis of ID dependencies.

This type of tool can be used in support of module 3 of the methodology. They could indeed be populated on one hand with the weakness of a given system or element (among its various attribute), on the other hand with the threatening element (i.e. GPS jammers), the kind of affected elements and the severity of effects. By matching both, it may infer the vulnerabilities. In addition, based on the relationships as stated above tool is able not only to infer the chains of indirect effects but also to find alternative solutions to mitigate these indirect effects.

[28] The conceptual framework is described in further detail in the MNE 7 Outcome 4 Conceptual and Pre-Doctrinal Paper: "Understanding Inter-Domain Dependencies and Vulnerabilities"; 31 January 2013.

Appendix D: Key Terms

This appendix defines the key terms to be used to consider ID issues and explains the linkages between them. The figure below provides a visualization of these terms and the relationships between them.

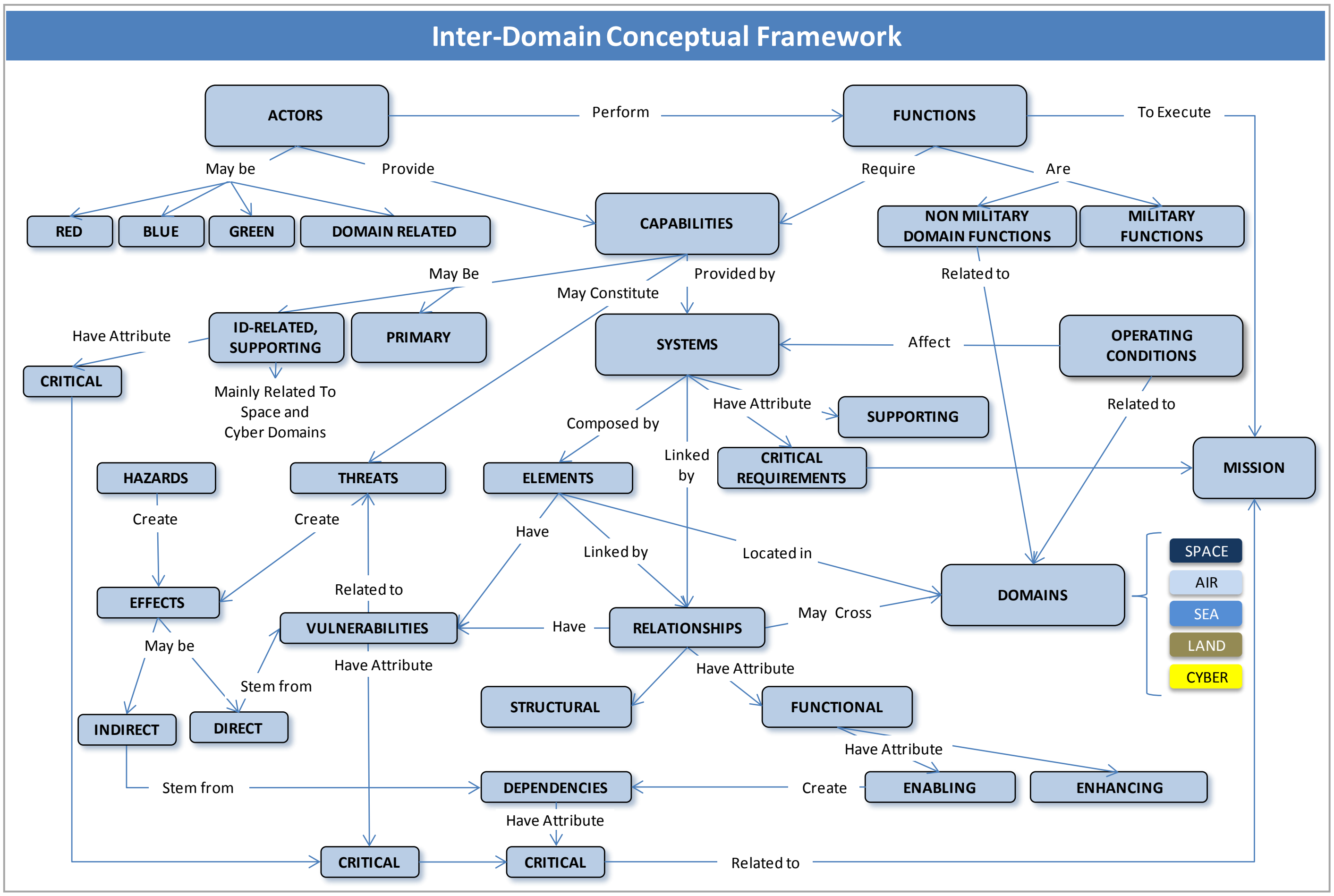


Figure 28: Inter-Domain (ID) Conceptual Framework.

Each key term of this inter-domain framework is defined below.

Actors

All parties and stakeholders that are part of the operational environment and either directly or indirectly have a share, take part, or influence the outcome of an engagement

The actors to be considered in an ID System include:

- The Blue (partners);
- The Red (potential or designated adversary);
- The Green actors, (non-aligned entities);
- The civilian "domain-related actors" of the area whose activities in one domain have a strong inter-domain dimension. They operate in and/or regulate the various domains and can be a sub-set of the previous categories.

Capability

The output that can be delivered by a combination of Doctrine, Organization, Training, Materiel, Leadership development, Personnel, Facilities and Interoperability (DOTMLPFI) resources. Most capabilities have an inter-domain dimension.

Center of Gravity (CoG)

The source of power that provides moral or physical strength, freedom of action, or will to act[29]

CoG Critical Capability

An ability that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s)

CoG Critical Requirement

The specific conditions, components or resources that are essential to sustaining those [critical] capabilities[30]

CoG Critical Vulnerability

An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects[31]

Critical

Something essential to the accomplishment of the specified or assumed objective(s)

[29] US JP-5

[30] COPD

[31] US JP 5-0

Critical ID Dependency

An inter-domain dependency which is essential to the achievement of the mission. Critical ID dependencies are to be themselves considered as a complementary subset of the critical requirements of the center of gravity.

Critical ID Vulnerability

The vulnerability of a system that constitutes a critical ID dependency (due to the fact that it is essential to the achievement of the mission). By extension, in this guide, to facilitate the formulation, the critical ID vulnerability designates the system itself.

Critical ID-related Supporting capability

The capabilities provided by ID systems, not specific to a military function, that enable the primary capabilities and which are essential to the accomplishment of the specified or assumed objective(s).

Domain

An area (maritime, air, space, land and cyberspace, the latter including physical and virtual dimensions) characterized by a specific geographical and/or technical environment.

Effect

The physical or behavioral state of a system that results from an action, a set of actions, or another effect. This guide distinguishes between direct effect and indirect effects:

- A direct effect results from an action or a set of actions, on a given system.
- An indirect effect results from another effect. There can be chains of indirect effects (including 2nd, 3rd, 4th, nth order effects)

Element of an Inter-Domain System

A specific physical, functional, or behavioral entity of an ID System. An element of an ID System can be resident in one or more domains and may be a space, air, maritime, land and cyber asset. Depending on the level of granularity, an element may be itself decomposed as a system, which may be inter-domain.

Enabler

An element, system, or operating condition that makes feasible or possible the ability of another element or system to accomplish its expected task as intended

Enabling Relationship

A functional relationship through which an element, system, or operating condition makes feasible or possible the ability of another element to accomplish its expected task as intended

Enhancer

An element, system, or operating condition that improves the ability of another element or system to accomplish its expected task as intended

Enhancing Relationship

A functional relationship through which an element, system, or operating condition improve the ability of another element to accomplish its expected task as intended

Hazard

An actual or potential non-hostile action or condition which may cause negative effect to an element or a relationship of the ID System

ID-Related Supporting Capability

The capabilities provided by ID systems and that enable the primary capabilities and are not specific to a military function. The basic supporting capabilities are:

- Communications, which may be decomposed into: Beyond Line of Sight (BLOS), Line of Sight (LOS) and Wired Communications;
- Positioning, Navigation and Timing (PNT)
- Information Management
- Remote Sensing

Note that the "primary" or "ID-related supporting nature of a capability, notable for information management and remote sensing, may differ according to the circumstances, the considered systems and doctrines.

ID Relationship

The connection between two elements of an ID system. They may be structural, functional or behavioral

Inter-Domain

Qualifier for something related to two or more different domains

Inter-Domain Dependency

The state, for a system element, of being solely reliant for support on another system element located in another domain. Dependency is related to a specific context and is relative to a technical, operational or functional need. By extension, in this guide, to facilitate the formulation, the ID dependency designates the element which provides this single enabling relationship.

Inter-Domain System

The functionally, physically or behaviorally related group of elements forming a unified whole, which dynamically connects the different domains and allows the interactions between capabilities and activities of these domains. The boundary of an Inter-Domain System is context-specific; thus, a different Inter-Domain System can be identified for each engagement.

Military Functions

The related capabilities and activities grouped together to help joint force commanders synchronize, integrate, and direct joint operations[32]. Also called "Joint Functions" in U.S. joint doctrine. These Military Functions are: Command and Control, Intelligence, Fires, Movement and Maneuver, Protection, and Sustainment.

Non-Military Domain Functions

The non-military activities and capabilities that take place in the domains [of the Global Commons] as related to an area of interest. They include primarily the access, use of, transit and exploitation of resources in each domain.

Operating conditions

Those conditions of each engagement which stem from the operational environment and other mission-related factors, such as the constraints and restraints, and which may determine and/or affect ID System, elements or relationships.

Primary Capability

The capabilities that directly ensure a specific military function (e.g. collection capabilities for the intelligence function, interdiction for the fires function)

Supporting Systems

The systems or assets providing an ID-related supporting capability. From a functional perspective, it includes the "enablers" and "enhancers"

Threat

The combination of implied or expressed intentions, capabilities, and willingness of one actor to negatively affect another actor and its assets

Vulnerability

The characteristics of a system that render it open to exploitation or susceptible to a given hazard or threat, possibly resulting in an impaired capability to perform a designated task

[32] US Joint Publication 3-0, *Joint Operations*, 11 August 2011, p III-1, definition of "joint function"

Intentionally Blank

Points of Contact

Lt Col Philippe COQUET
MNE 7 FRA National Director
Centre Interarmées de Concepts, de Doctrines et d'Expérimentations
E-mail: philippe.coquet@intradef.gouv.fr
Phone: + 33 1 44 42 82 71

Mr. Philippe GROS
MNE 7 Outcome 4 Concept Developer
Fondation pour la recherche stratégique
E-mail: p.gros@frstrategie.org
Mobile Phone: + 33 6 16 61 04 02
Work Phone: + 33 1 43 13 77 87

Mrs. Anne KOVACS
MNE 7 Outcome 4 Project Lead
U.S.-CREST
E-mail: anne.kovacs@uscrest.org
Phone : + 1 703 243 6908

Mr. Dominique ORSINI
MNE 7 FRA Lead Analyst
U.S.-CREST
E-mail: dorsini@uscrest.org
Phone: + 1 703 243 6908